EXHIBIT B

Deloitte.

Deloitte & Touche LLP
555 Mission Street
Suite 1400
San Francisco, CA 94105
USA

Tel:+1 415 783 4000
www.deloitte.com

December 10, 2019

Ms. Dominique Mielle
Chair
The Audit Committee of PG&E Corporation and
The Audit Committee of Pacific Gas and Electric Company
77 Beale Street
San Francisco, CA 94105

Mr. David S. Thomason
Vice President and Controller
PG&E Corporation
Vice President, Controller and Chief Financial Officer
Pacific Gas and Electric Company
77 Beale Street
San Francisco, CA 94105

Dear Ms. Mielle and Mr. Thomason:

Deloitte & Touche LLP ("D&T" or "we" or "us") is pleased to serve as the independent registered public accounting firm for PG&E Corporation and Pacific Gas and Electric Company (the "Utility") (each, the "Company" and collectively, the "Companies" or "you" or "your"). Mr. Timothy Gillam will be responsible for the services that we perform for the Companies hereunder.

In addition to the audit and review services we are engaged to provide under this engagement letter, we would also be pleased to assist the Companies on issues as they arise throughout the year. Hence, we hope that you will call Mr. Gillam whenever you believe D&T can be of assistance. This assistance will require approval by the Companies' Audit Committees (each the "Audit Committee" and collectively, the "Audit Committees") in accordance with their preapproval policies and procedures.

The services to be performed by D&T pursuant to this engagement are subject to the terms and conditions set forth herein and in the accompanying appendices. Such terms and conditions shall be effective as of the date of the commencement of such services.

Audit of Financial Statements and the Effectiveness of Internal Control over Financial Reporting

Our engagement is to perform an integrated audit in accordance with the standards of the Public Company Accounting Oversight Board (PCAOB) (United States) (the "PCAOB Standards"). The objectives of an integrated audit conducted in accordance with the PCAOB Standards are the expression of opinions on (1) the fairness of the presentation of each of the Companies' consolidated financial statements for the year ending December 31, 2020, (the "consolidated financial statements") in conformity with accounting principles generally accepted in the United States of America ("generally accepted accounting principles"), in all material respects, and (2) the effectiveness of each of the Companies' internal control over financial reporting as of December 31, 2020, based on the criteria established in *Internal Control — Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (the "COSO Framework").

Appendix A contains a description of an integrated audit in accordance with the PCAOB Standards.

Our ability to express any opinion or to issue any report as a result of this engagement and the wording thereof will, of course, be dependent on the facts and circumstances at the date of our reports. If, for any reason, we are unable to complete our audit or are unable to form or have not formed any opinion, we may decline to express any opinion or decline to issue any report as a result of this engagement. If we are unable to complete our audit, or if any report to be issued by D&T as a result of this engagement requires modification, the reasons for this will be discussed with the applicable Company's Audit Committee and the Companies' management.

Audit of Financial Statements in Accordance with the Accounting Requirements of the Federal Energy Regulatory Commission Form 1

Our engagement is also to perform an audit of the Utility's consolidated regulatory-basis financial statements included within its Federal Energy Regulatory Commission ("FERC") Form 1 filing for the year ending December 31, 2020 (the "regulatory-basis financial statements") in accordance with auditing standards generally accepted in the United States of America ("generally accepted auditing standards") (hereinafter, the "FERC audit"). The objective of an audit conducted in accordance with generally accepted auditing standards is to express an opinion on whether the Utility's regulatory-basis financial statements for the year ending December 31, 2020, are presented fairly, in all material respects, in accordance with the accounting requirements of the FERC as set forth in its applicable Uniform System of Accounts and published accounting releases, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America (the "FERC accounting requirements").

Appendix B contains a description of the auditor's responsibilities and the scope of an audit in accordance with generally accepted auditing standards.

We expect to issue a written report upon the completion of our FERC audit. Our ability to express an opinion or to issue any report as a result of this engagement and the wording thereof will, of course, be dependent on the facts and circumstances at the date of our report. If, for any reason, we are unable to complete our audit or are unable to form or have not formed an opinion, we may decline to express an opinion or decline to issue any report as a result of this engagement. If we are unable to complete our audit or if any report to be issued by D&T as a result of this engagement requires modification, the reasons for this will be discussed with the Utility's Audit Committee and management.

Reviews of Interim Financial Information

We will also perform a review of the Companies' condensed interim financial information (the "interim financial information") in accordance with the PCAOB Standards ("interim review") for each of the quarters in the year ending December 31, 2020, prepared for submission to the Securities and Exchange Commission (SEC). The objective of an interim review is to provide us with a basis for communicating whether we are aware of any material modifications that should be made to the interim financial information for it to conform with generally accepted accounting principles. The objective of an interim review is also to provide us with a basis for determining whether we are aware of any material modifications that, in our judgment, should be made to management's disclosures about changes in internal control over financial reporting that have materially affected or are reasonably likely to materially affect the Companies' internal control over financial reporting for management's certifications to be accurate and to comply with the requirements of Section 302 of the Sarbanes-Oxley Act of 2002 and related SEC rules and regulations.

Appendix A also contains a description of an interim review in accordance with the PCAOB Standards.

If we become aware of material modifications that should be made to the interim financial information for it to conform with generally accepted accounting principles, or if we become aware of deficiencies in internal control over financial reporting so significant that they would preclude management's preparation of interim financial information in conformity with generally accepted accounting principles, we may be precluded from completing any of our reviews and, accordingly, we would be unable to issue a review report on the interim financial information. If, for any reason, we are unable to complete any of our interim reviews, the reasons for this will be discussed with the applicable Company's Audit Committee and the Companies' management.

Management's Responsibilities

Appendix C describes management's responsibilities.

Audit Committees' Responsibility and Auditor Communications

As the independent registered public accounting firm of the Companies, we acknowledge that each Company's Audit Committee is directly responsible for the appointment, compensation, and oversight of our work, and accordingly, except as otherwise specifically noted, we will report directly to the Audit Committees. You have advised us that the services to be performed under this engagement letter, including, where applicable, the use by D&T of affiliates or related entities as subcontractors in connection with this engagement, have been approved by the Audit Committees in accordance with the Audit Committees' established preapproval policies and procedures.

Under the PCAOB Standards and SEC Rule 2-07 of Regulation S-X, we are required to communicate with the respective Audit Committee about various matters in connection with our audit and interim reviews. Appendix D describes such communications.

Fees

We estimate that our fees for the audits of each Company's consolidated financial statements, the reviews of the related interim financial information, the audits of each Company's internal control over financial reporting, and the Utility's FERC Form 1 audit for the year ending December 31, 2020 will be $680,000, plus expenses for PG&E Corporation and $3,800,000, plus expenses, for Pacific Gas and Electric Company. Based on the anticipated timing of the work, our fees for the audits of each Company's consolidated financial statements, the reviews of the related interim financial information, the audits of each Company's internal control over financial reporting, and the Utility's FERC Form 1 audit for the year ending December 31, 2020 will be billed monthly.

Subject to any applicable Bankruptcy Court (as defined below) order, rules or procedures, and payments are due 45 days after the receipt of the invoice. Engagement-related expenses, such as travel, printing, postage, administrative costs, and technology and administrative-related charges will be billed in addition to the fees and will be stated separately on the invoices.

Our continued service on this engagement is dependent upon payment of our invoices in accordance with these terms. Our estimated fees are based on certain assumptions, including (1) timely and accurate completion of the requested entity participation schedules and additional supporting information, (2) no inefficiencies during the audit or interim review process or changes in scope caused by events that are beyond our control, (3) the effectiveness of internal control over financial reporting throughout the periods under audit and interim review, (4) a minimal level of audit adjustments (recorded or unrecorded), and (5) no changes to the timing or extent of our work plans. We will notify you promptly of any

circumstances we encounter that could significantly affect our estimate and discuss with you any additional fees, as necessary.

To the extent that any of the assumptions listed above are not realized or if we are requested to provide additional audit-related services including consultation on accounting and financial reporting issues such as those related to regulatory, transactional and SEC matters, fees for such services will be based on standard rates and hours incurred. These situations will be discussed with you on a timely basis, and any additional billings will be billed separately. Accounting consultations on accounting and financial reporting matters are not included in the fees above, however, they are pre-approved for the year ending December 31, 2020 up to $25,000 for PG&E Corporation and $75,000 for Pacific Gas and Electric Company.

Chapter 11 Proceeding

With respect to services performed prior to the date of each Company's emergence from its Chapter 11 proceeding, D&T expects to apply for compensation for professional services rendered and for reimbursement of expenses incurred, in accordance with applicable provisions of title 11 of the United States Code (the "Bankruptcy Code"), the Federal Rules of Bankruptcy Procedure, the applicable local rules of bankruptcy procedure (the "Local Rules"), the United States Bankruptcy Court Northern District of California Guidelines for Compensation and Expense Reimbursement of Professionals and Trustees, effective February 19, 2014, and the United States Trustee Guidelines for Reviewing Applications for Compensation and Reimbursement of Expenses Filed under Bankruptcy Code § 330 (collectively, the "Fee Guidelines", and any further orders of the Bankruptcy Court regarding the payment of fees and reimbursement of expenses of professionals (the "Orders"). In such event, payment of fees and reimbursement of expenses will be subject to ultimate allowance and approval by the Bankruptcy Court. However, in the interim, each Company will ask the Bankruptcy Court for approval to allow D&T to submit invoices to each Company for prompt payment in accordance with the Local Rules, the Fee Guidelines, and the Orders. If applicable, payment of these invoices will be made by each Company on an interim basis subject to approval and allowance upon application to and order by the Bankruptcy Court.

Each Company agrees that it will promptly seek the Bankruptcy Court's approval of this engagement and the Engagement Letter. The application, proposed order and other supporting documents (collectively, the "Application") submitted to the Bankruptcy Court seeking its approval of this engagement must be reasonably satisfactory to D&T in all respects. In addition to D&T's other rights or remedies hereunder, D&T may, in its sole discretion and without any liability arising there from, terminate this engagement in the event that (a) a third party files a formal written objection with the Bankruptcy Court to D&T's retention by each Company on the terms and conditions set forth in this Engagement Letter, (b) a final order authorizing the employment of D&T is not issued by the Bankruptcy Court on or before thirty (30) days from the filing date of the Application, or (c) the Application is denied by the Bankruptcy Court; provided that, in the case of (a) or (b), D&T provides each Company with three (3) days' written notice prior to terminating this engagement as a result of any of the aforementioned events. In any such event, each Company hereby agrees to withdraw or amend, promptly upon D&T's request, any Application filed or to be filed with the Bankruptcy Court to retain D&T's services in the Chapter 11 proceeding.

For purposes of this Engagement Letter, together with the General Business Terms and Appendix E attached hereto, "Bankruptcy Court" shall mean the United States Bankruptcy Court with which each Company has filed a Chapter 11 petition.

Inclusion of D&T Reports or References to D&T in Other Documents or Electronic Sites

If either Company intends to publish or otherwise reproduce in any document any report issued as a result of this engagement, or otherwise make reference to D&T in a document that contains other information in addition to the audited consolidated financial statements (e.g., in a periodic filing with the SEC or other regulator, in a debt or equity offering circular, or in a private placement memorandum), thereby associating D&T with such document, the Company agrees that its management will provide D&T with a draft of the document to read and obtain our approval for the inclusion or incorporation by reference of any of our reports, or the reference to D&T, in such document before the document is printed and distributed. The inclusion or incorporation by reference of any of our reports in any such document would constitute the reissuance of such reports. The Company also agrees that its management will notify us and obtain our approval prior to including any of our reports on an electronic site.

Our engagement to perform the services described herein does not constitute our agreement to be associated with any such documents published or reproduced by or on behalf of the Company. Any request by either Company to reissue any report issued as a result of this engagement, to consent to any such report's inclusion or incorporation by reference in an offering or other document, or to agree to any such report's inclusion on an electronic site will be considered based on the facts and circumstances existing at the time of such request. The estimated fees outlined herein do not include any procedures that would need to be performed in connection with any such request. Should D&T agree to perform such procedures, fees for such procedures would be subject to the mutual agreement of the Company and D&T.

Restriction on Report Use

The Utility agrees that any attest report issued by D&T on regulatory-basis financial statements included within the FERC filing is intended solely for the information and use of the Audit Committee, management of the Utility and for filing with the Federal Energy Regulatory Commission, and that our report is not intended to be and should not be used by anyone other than these specified parties; nor will it be made available to any other persons or entities, or included, incorporated by reference, or referred to in any filings with regulators except for filing with the Federal Energy Regulatory Commission.

Other Services

For preapproval purposes, this engagement letter also acknowledges that D&T may be asked to provide certain other services. These services include:

- The issuance of a "comfort letter" related to anticipated offerings of debt or equity during 2020. Certain procedures will be performed on a quarterly basis to expedite the issuance of a comfort letter if one is ultimately required. The procedures for such comfort letters will ultimately be determined by the underwriters and agreed to by D&T. We estimate fees for comfort letters will approximate $45,000 per letter.

- The issuance of a consent letter for the reissuance of reports during 2020. Fees for procedures related to consents to reissue reports will approximate $25,000 each time consent is required.

- The fees related to the issuance of comfort letters and consent letters discussed above are pre-approved for the year ending December 31, 2020, up to $420,000 for PG&E Corporation and $350,000 for Pacific Gas and Electric Company.

- Outside-of-engagement scope audit procedures (including, for example performing audit procedures in connection with statutory or regulatory filings, engagements and regulatory reviews of audit workpapers, specific transactions/accounting, reporting on critical audit matters, adoption of new accounting pronouncements, internal controls surrounding new applications, systems or activities, and changes in laws or regulations in the current year). Fees for such services will be billed based on standard rates and hours incurred; for the year ending December 31, 2020, these fees are pre-approved up to $2,270,000.

- Other audit-related services (including, for example, agreed-upon procedures, advice and recommendations regarding proposed transactions, adoption of new accounting pronouncements, internal controls surrounding new applications, systems or activities, and training in a future year). Fees for such services will be based on standard rates and hours incurred; for the year ending December 31, 2020, these fees are pre-approved up to $800,000.

In addition, we acknowledge that we provide the following recurring services, which are not described herein as they are governed by separate engagement letters:

- The financial statement audits of the Nuclear Facilities Non-Qualified CPUC Decommissioning Master Trust, the Nuclear Facilities Qualified CPUC Decommissioning Master Trust, and the Nuclear Facilities Qualified FERC Decommissioning Master Trust of Pacific Gas and Electric Company. Fees are estimated to be $75,000.

* * * * * *

The parties acknowledge and agree that D&T is being engaged under this engagement letter to provide only the services described herein. Should any of the Companies or the Audit Committees request, and should D&T agree to provide, services (including audit services) beyond those described herein, such services will constitute a separate engagement and will be governed by a separate engagement letter.

This engagement letter, including Appendices A through G attached hereto and made a part hereof, constitutes the entire agreement between the parties with respect to this engagement and supersedes any other prior or contemporaneous agreements or understandings between the parties, whether written or oral, relating to this engagement.

If the above terms are acceptable and the services described are in accordance with your understanding, please sign the copy of this engagement letter in the space provided and return it to us.

Yours truly,

Deloitte & Touche LLP

Acknowledged and agreed to on behalf of
the Audit Committee of PG&E Corporation and
the Audit Committee of Pacific Gas and Electric Company:

By: Dominique Mielle DOMINIQUE MIELE

Title: Chair, Audit Committee

Date: 1/17/2020

Accepted and agreed to by
PG&E Corporation and Pacific Gas and Electric Company:

By: David Thomason

Title: Vice President & Controller, Utility CFO

Date: 1/14/20

APPENDIX A

DESCRIPTION OF AN INTEGRATED AUDIT AND INTERIM REVIEW IN ACCORDANCE WITH THE PCAOB STANDARDS

This Appendix A is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

Components of an Integrated Audit

An integrated audit includes the following:

- Examining, on a test basis, evidence supporting the amounts and disclosures in the consolidated financial statements
- Inquiring directly of each Audit Committee regarding (1) its views about fraud risks in the applicable Company, (2) whether it has knowledge of any actual, suspected, or alleged fraud affecting the applicable Company, and (3) whether it is aware of tips or complaints regarding the applicable Company's financial reporting (including those received through any internal whistleblower program, if such program exists) and, if so, its responses to such tips and complaints
- Assessing the accounting principles used and significant estimates made by management
- Evaluating the overall financial statement presentation
- Examining, on a test basis, evidence supporting the design and operating effectiveness of each Company's internal control over financial reporting
- Evaluating the effectiveness of each Company's internal control over financial reporting

An integrated audit does not include the performance of any procedures with respect to financial information in an interactive data format using eXtensible Business Reporting Language (XBRL). Any procedures that the Companies request D&T to perform related to any such XBRL interactive data would be described in a separate engagement letter.

Reasonable Assurance

The PCAOB Standards require that we plan and perform the audits to obtain reasonable, rather than absolute, assurance about (1) whether the consolidated financial statements are free of material misstatement, whether caused by error or fraud, and (2) whether effective internal control over financial reporting was maintained in all material respects. However, because of the characteristics of fraud, a properly planned and performed audit may not detect a material misstatement or material weakness. Accordingly, there is some risk that a material misstatement of the consolidated financial statements or a material weakness in internal control over financial reporting would remain undetected. Also, an integrated audit is not designed to detect error or fraud that is immaterial to the consolidated financial statements or deficiencies in internal control over financial reporting that, individually or in combination, are less severe than a material weakness.

Inherent Limitations of Internal Control over Financial Reporting

Because of the inherent limitations of internal control over financial reporting, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Interim Reviews

An interim review is substantially less in scope than an audit in accordance with the PCAOB Standards, the objective of which is to express an opinion on the financial statements taken as a whole. Accordingly, an interim review will not result in the expression of an opinion concerning the fairness of the presentation of the interim financial information in conformity with generally accepted accounting principles and cannot be relied on to reveal all significant matters that would be disclosed in an audit.

An interim review consists principally of applying analytical procedures to pertinent financial data and making inquiries of, and evaluating responses from, certain management personnel of the Companies who have responsibility for financial and accounting matters. An interim review also includes obtaining sufficient knowledge of the Companies' business and their internal control as they relate to the preparation of both annual and interim financial information to (1) identify the types of potential material misstatements in the interim financial information and consider the likelihood of their occurrence, and (2) select the inquiries and analytical procedures that will provide us with a basis for communicating whether we are aware of any material modifications that should be made to the interim financial information for it to conform with generally accepted accounting principles. An interim review is not designed to provide assurance on internal control or to identify control deficiencies.

An interim review does not include the performance of any procedures with respect to interim financial information in an interactive data format using XBRL.

An interim review also includes procedures, principally observation and inquiries, relating to management's disclosures about changes in internal control over financial reporting to provide us with a basis for communicating whether we are aware of any modifications that, in our judgment, should be made to such disclosures for management's certifications to be accurate and to comply with the requirements of Section 302 of the Sarbanes-Oxley Act of 2002 and related SEC rules and regulations. These procedures are substantially less in scope than an audit of internal control over financial reporting in accordance with the PCAOB Standards. Accordingly, an interim review cannot be relied on to reveal all significant matters that would be disclosed in an audit of internal control over financial reporting, and we will not express an opinion on the effectiveness of internal control over financial reporting.

APPENDIX B

AUDITOR'S RESPONSIBILITIES AND SCOPE OF AN AUDIT IN ACCORDANCE WITH GENERALLY ACCEPTED AUDITING STANDARDS FOR THE AUDIT OF FINANCIAL STATEMENTS IN ACCORDANCE WITH THE ACCOUNTING REQUIREMENTS OF THE FEDERAL ENERGY REGULATORY COMMISSION FORM 1

This Appendix B is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

Auditor's Responsibilities

Our responsibilities under generally accepted auditing standards include forming and expressing an opinion about whether the regulatory-basis financial statements that have been prepared by the Utility's management with the oversight of the Utility's Audit Committee are presented fairly, in all material respects, in accordance with the FERC accounting requirements. The audit of the regulatory-basis financial statements does not relieve the Utility's management or the Utility's Audit Committee of their responsibilities.

Scope of an Audit

Generally accepted auditing standards require that we plan and perform the audit to obtain reasonable, rather than absolute, assurance about whether the regulatory-basis financial statements as a whole are free from material misstatements, whether caused by fraud or error. However, because of the inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk exists that some material misstatements may not be detected, even though the audit is properly planned and performed in accordance with generally accepted auditing standards. We have no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by fraud or error, that are not material to the regulatory-basis financial statements as a whole are detected.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the regulatory-basis financial statements. The procedures selected depend on our judgement, including the assessment of the risks of material misstatements of the regulatory-basis financial statements, whether caused by fraud or error. In making those risk assessments, we consider internal control relevant to the Utility's preparation and fair presentation of the regulatory-basis financial statements in order to design audit procedures that are appropriate in the circumstances but not for the purpose of expressing an opinion on the effectiveness of the Utility's internal control. An audit also includes evaluating the appropriateness of accounting policies used, and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the regulatory-basis financial statements.

APPENDIX C

MANAGEMENT'S RESPONSIBILITIES

This Appendix C is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

Financial Statements and the Effectiveness of Internal Control over Financial Reporting

Management is responsible for the preparation, fair presentation, and overall accuracy of the consolidated financial statements and interim financial information, including disclosures, in conformity with generally accepted accounting principles and regulatory-basis financial statements in conformity with FERC accounting requirements, as applicable. The assessment of the effectiveness of internal control over financial reporting to comply with Section 404 of the Sarbanes-Oxley Act of 2002 and related SEC rules and regulations is also the responsibility of management. In this regard, management has the responsibility for, among other things:

- Selecting and applying the accounting policies
- Establishing and maintaining effective internal control over financial reporting and informing D&T of all deficiencies in the design or operation of internal control over financial reporting identified as part of management's evaluation, including separately disclosing to D&T all such deficiencies that management believes to be significant deficiencies or material weaknesses in internal control over financial reporting
- Informing D&T of significant changes in the design or operation of each Company's internal control over financial reporting that occurred during each fiscal quarter or subsequent to the date being reported on
- Identifying and ensuring that the Companies comply with the laws and regulations applicable to their activities and informing us of any known or possible material violations of such laws or regulations
- Adjusting the financial statements to correct material misstatements relating to accounts or disclosures, and affirming to D&T in the representation letter that the effects of any uncorrected misstatements aggregated by us are immaterial, both individually and in the aggregate, to the consolidated financial statements and the regulatory-basis financial statements taken as a whole
- Providing D&T with (1) access to all information of which management and, where appropriate, the Audit Committees are aware that is relevant to the preparation and fair presentation of the consolidated financial statements and the regulatory-basis financial statements, such as records, documentation, and other matters, (2) additional information that we may request from management and, where appropriate, the Audit Committees for the purpose of our audit, and (3) unrestricted access to personnel within the Companies from whom we determine it necessary to obtain evidence
- Including all informative disclosures in the regulatory-basis financial statements that are appropriate for the purpose of complying with the accounting requirements of

the FERC as set forth in its applicable Uniform System of Accounts and published accounting releases.

Management's Representations

We will make specific inquiries of the Companies' management about the representations embodied in the consolidated financial statements and regulatory-basis financial statements and management's assessment of the effectiveness of the Companies' internal control over financial reporting. In addition, we will request that management provide us with the written representations the Companies are required to provide to their independent registered public accounting firm under the PCAOB Standards and generally accepted auditing standards. The responses to those inquiries and the written representations of management are part of the evidential matter that D&T will rely on in forming its opinions. We will also request a similar representation letter as part of our interim reviews.

Process for Obtaining Preapproval of Services

Management is responsible for the coordination of obtaining the preapproval of the Audit Committees, in accordance with the Audit Committees' preapproval process, for any services to be provided by D&T to the Companies.

Program and Subscription Services

D&T makes available to clients and nonclients various educational and informational programs, seminars, tools, and related services, such as live programs, webcasts (including the Dbriefs webcast series), podcasts, websites, database subscriptions (including some that provide access to D&T proprietary information and tools that offer technical support and advice), checklists, research reports, surveys, published books and other materials, applications, local office seminars, Technical Library, and CXO conferences (collectively, "programs and subscriptions"). D&T may provide these programs and subscriptions free of charge, for a nominal fee, or for a fee at prevailing market rates. In some instances, D&T may include complimentary rooms or meals as part of programs or seminars. Any programs and subscriptions requested by the Companies or their affiliates and the related fees (if any) would be subject to the mutual agreement of the Companies or their affiliates, as applicable, and D&T and may be described in a separate written agreement. The Companies hereby confirm that any use or receipt by the Companies or their affiliates of these programs and subscriptions is approved by the Audit Committees in accordance with any applicable requirements in the Audit Committees' established preapproval policies and procedures.

Independence Matters

In connection with our engagement, D&T, management, and the Audit Committees will assume certain roles and responsibilities in an effort to assist D&T in maintaining independence and ensuring compliance with the securities laws and regulations. D&T will communicate to its partners, principals, and employees that the Companies are attest clients. Management of the Companies will ensure that the Companies, together with their subsidiaries and other entities that comprise the Companies for purposes of the consolidated financial statements, have policies and procedures in place for the purpose of ensuring that neither the Companies nor any such subsidiary or other entity will act to engage D&T or accept from D&T any service that either has not been subjected to their preapproval process or that under SEC or other applicable rules would impair D&T's independence. All potential services are to be discussed with Mr. Gillam.

In connection with the foregoing, the Companies agree to furnish to D&T and keep D&T updated with respect to (1) a corporate tree that identifies the legal names of the Companies'

affiliates, including affiliates as defined in SEC Rule 2-01(f)(4) of Regulation S-X, (e.g., parents, subsidiaries, investors, or investees), together with the ownership relationship among such entities, and (2) any equity or debt securities of the Companies and their affiliates (including, without limitation, tax-advantaged debt of such entities that is issued through governmental authorities) that are available to individual investors (whether through stock, bond, commodity, futures or similar markets in or outside of the United States, or equity, debt, or any other securities offerings), together with related securities identification information (e.g., ticker symbols or CUSIP®, ISIN®, or Sedol® numbers). The Companies acknowledge and consent that such information may be treated by D&T as being in the public domain.

Management will coordinate with D&T to ensure that D&T's independence is not impaired by hiring former or current D&T partners, principals, or professional employees for certain positions. Management of the Companies will ensure that the Companies, together with their subsidiaries and other entities that comprise the Companies for purposes of the consolidated financial statements, also have policies and procedures in place for purposes of ensuring that D&T's independence will not be impaired by hiring a former or current D&T partner, principal, or professional employee in an accounting role or financial reporting oversight role that would cause a violation of securities laws and regulations. Any employment opportunities with the Companies for a former or current D&T partner, principal, or professional employee should be discussed with Mr. Gillam and approved by the Audit Committees before entering into substantive employment conversations with the former or current D&T partner, principal, or professional employee, if such opportunity relates to serving (1) as chief executive officer, controller, chief financial officer, chief accounting officer, or any equivalent position for either Company or in a comparable position at a significant subsidiary of either Company; (2) on either Company's board of directors; (3) as a member of either Company's Audit Committee; or (4) in any other position that would cause a violation of securities laws and regulations.

For purposes of the preceding five paragraphs, "D&T" shall mean Deloitte & Touche LLP and its subsidiaries; Deloitte Touche Tohmatsu Limited, its member firms, the affiliates of Deloitte & Touche LLP, Deloitte Touche Tohmatsu Limited and its member firms; and, in all cases, any successor or assignee.

APPENDIX D

COMMUNICATIONS WITH THE AUDIT COMMITTEE

This Appendix D is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

Independence Communications

We have the responsibility to comply with the rules and standards of the PCAOB and the securities laws and regulations administered by the SEC regarding auditor independence. To demonstrate compliance with those requirements and in accordance with PCAOB Ethics and Independence Rule 3526, *Communication with Audit Committees Concerning Independence* ("Rule 3526"), we will describe to the Audit Committees, in writing, all relationships between D&T and the Companies, their affiliates, or persons in "financial reporting oversight roles" (as defined in SEC Rule 2-01 of Regulation S-X) at the Companies, that may reasonably be thought to bear on our independence and affirm to the Audit Committees in such communication whether we are independent of the Companies within the meaning of the rules and standards of the PCAOB and the securities laws and regulations administered by the SEC. We also will discuss our independence with the Audit Committees in accordance with Rule 3526. For purposes of this paragraph, "D&T" shall mean Deloitte & Touche LLP and its subsidiaries; Deloitte Touche Tohmatsu Limited, its member firms, the affiliates of Deloitte & Touche LLP, Deloitte Touche Tohmatsu Limited and its member firms; and, in all cases, any successor or assignee.

Other Communications Arising from the Audit or Interim Reviews

Fraud and Illegal Acts

We will report directly to the Audit Committees any fraud of which we become aware that involves senior management and any fraud (whether caused by senior management or other employees) of which we become aware that causes a material misstatement of the consolidated financial statements. We will report to senior management any fraud perpetrated by lower level employees of which we become aware that does not cause a material misstatement of the consolidated financial statements; however, we will not report such matters directly to the Audit Committees, unless otherwise directed by the Audit Committees.

We will inform the appropriate level of management of the Companies and determine that the Audit Committees are adequately informed with respect to illegal acts that have been detected or have otherwise come to our attention during the course of our audit, unless the illegal acts are clearly inconsequential.

Internal Control Matters

We will communicate in writing to management and the Audit Committees all material weaknesses (as defined in the PCAOB Standards or generally accepted auditing standards, as applicable) identified during the audit. We will also communicate in writing to the Audit Committees all significant deficiencies (as defined in the PCAOB Standards or generally accepted auditing standards, as applicable) identified during the audit. If we conclude that the oversight of the Companies' external financial reporting and internal control over financial reporting by the Audit Committees are ineffective, we will also communicate that conclusion in writing to the Companies' boards of directors.

In addition, for the integrated audit, we will communicate to management in writing all deficiencies in internal control over financial reporting (i.e., those deficiencies in internal control over financial reporting that are of a lesser magnitude than material weaknesses) identified during the audits and inform the Audit Committees when such communication has been made. When making this communication, we will not repeat information about deficiencies that has been included in previously issued written communications, whether those communications were made by us, internal auditors, or others within the Companies.

We will also communicate in writing to management and the Audit Committee any significant deficiencies or material weaknesses in internal control (as defined in generally accepted auditing standards) that we have identified during the audit of financial statements in accordance with the accounting requirements of the FERC Form 1, including those that were remediated during the audit.

Other Matters

We will communicate matters required by PCAOB Auditing Standard 1301, *Communications with Audit Committees*, and SEC Rule 2-07 of Regulation S-X prior to the Companies filing our report or consent with the SEC.

In addition, at the request of either Audit Committee, we will provide the Audit Committees with a report in connection with the New York Stock Exchange Corporate Governance Listing Standards.

We are also responsible for communicating with the Audit Committee significant matters related to the audit of financial statements in accordance with the accounting requirements of the FERC Form 1 that are, in our professional judgment, relevant to the responsibilities of the Audit Committee in overseeing the financial reporting process. Generally accepted auditing standards do not require us to design procedures for the purpose of identifying other matters to communicate with the Audit Committee. However, we will communicate to the Audit Committee matters required by AICPA AU-C 260, The Auditor's Communication with Those Charged with Governance.

Interim Reviews

We will communicate to management and, if appropriate, the Audit Committees matters that cause us to believe that (1) material modifications should be made to the interim financial information for it to conform with generally accepted accounting principles, (2) modifications to management's disclosures about changes in internal control over financial reporting are necessary for management's certifications to be accurate and to comply with the requirements of Section 302 of the Sarbanes-Oxley Act of 2002 and related SEC rules and regulations, or (3) the Companies filed the Form 10-Q before the completion of our review. When conducting our interim reviews, we will also determine whether any other matters required by regulations or the PCAOB Standards as they relate to interim financial information have been identified. If such matters have been identified, we will communicate them to the Audit Committees prior to the filing of interim financial information with the SEC.

APPENDIX E

GENERAL BUSINESS TERMS

This Appendix E is part of the engagement letter to which these terms are attached (the engagement letter, including its appendices, the "engagement letter") dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

1. Independent Contractor. D&T is an independent contractor and D&T is not, and will not be considered to be, an agent, partner, fiduciary, or representative of the Companies or the Audit Committees.

2. Survival. The agreements and undertakings of the Companies and the Audit Committees contained in the engagement letter will survive the completion or termination of this engagement.

3. Assignment and Subcontracting. Except as provided below, no party may assign any of its rights or obligations (including, without limitation, interests or claims) relating to this engagement without the prior written consent of the other parties. The Companies and the Audit Committees hereby consent to D&T subcontracting a portion of its services under this engagement to any affiliate or related entity, whether located within or outside of the United States; provided, however that such subcontracting will not relieve D&T of any obligations to the Companies hereunder. Professional services performed hereunder by any of D&T's affiliates or related entities shall be invoiced as professional fees, and any related expenses shall be invoiced as expenses, unless otherwise agreed.

4. Severability. If any term of the engagement letter is unenforceable, such term shall not affect the other terms, but such unenforceable term shall be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permissible the intent of the parties set forth herein.

5. Force Majeure. No party shall be deemed to be in breach of the engagement letter as a result of any delays or non-performance directly or indirectly resulting from circumstances or causes beyond its reasonable control, including, without limitation, fire, epidemic or other casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority.

6. Confidentiality. To the extent that, in connection with this engagement, D&T comes into possession of any confidential information of the Companies, D&T shall not disclose such information to any third party without the Companies' consent, using at least the same degree of care as it employs in maintaining in confidence its own confidential information of a similar nature, but in no event less than a reasonable degree of care. The Companies and the Audit Committees hereby consent to D&T disclosing such information (1) as may be required by law or regulation, or to respond to governmental inquiries, or in accordance with applicable professional standards or rules, or in connection with litigation or arbitration pertaining hereto; (2) to the extent such information (i) is or becomes publicly available other than as the result of a disclosure in breach hereof, (ii) becomes available to D&T on a nonconfidential basis from a source that D&T believes is not prohibited from disclosing such information to D&T, (iii) is already known by D&T without any obligation of confidentiality with respect thereto, or (iv) is developed by D&T independently of any disclosures made to D&T hereunder; or (3) to contractors providing administrative, infrastructure, and other support services to D&T and subcontractors providing services in connection with this engagement, in each case, whether located within or outside of the United States, provided that such contractors and subcontractors

have agreed to be bound by confidentiality obligations similar to those in this paragraph. To the extent that any information obtained by D&T from or on behalf of the Companies or their employees in connection with the performance of services under the engagement letter relates to a resident of Massachusetts and constitutes "Personal Information" as defined in 201 CMR 17.02 (as may be amended), D&T shall comply with the obligations of 201 CMR 17.00 et. seq. (as may be amended), entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth," with respect to such information. D&T shall promptly notify the Companies if D&T becomes aware of any unauthorized access to or disclosure of confidential information of the Companies.

7. Third Party Information Technology Controls Reports. Deloitte LLP ("Deloitte U.S.") has engaged a third party (the "Service Provider") to (i) apply procedures based upon a version of the Shared Assessment Program Agreed Upon Procedures with respect to certain of Deloitte U.S.'s information technology controls and to prepare a report with respect thereto (the "Shared Assessments Report"), and (ii) conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability, established by the American Institute of Certified Public Accountants (AICPA) ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC 2 Report"). Upon written request, Deloitte U.S. shall promptly provide Client with one copy of (i) the Shared Assessments Report, provided that Client executes any documentation required by the Service Provider to become a specified user thereof, (ii) the SOC 2 Report, or (iii), a report prepared by a third party that is designed to provide similar information as such reports. Client shall not disclose such reports, or refer to such reports in any communication, to any person or entity other than Client. In the event that Client has any questions regarding such reports, Deloitte U.S. shall make appropriate personnel reasonably available to discuss the contents thereof.

8. Code of Ethics and Professional Conduct. We acknowledge that we maintain a Code of Ethics and Professional Conduct. The D&T Code of Ethics and Professional Conduct (the "Code") may be found on www.deloitte.com under the Code of Ethics and Professional Conduct section under the Ethics & Independence section under the About section on that web site. The Code states that it is the obligation of all D&T personnel to know, understand, and comply with this Code.

9. Background Check Contract Requirements. Deloitte LLP and its subsidiaries (collectively the "Deloitte U.S. Firms") generally require that background investigations be conducted for all employees, partners, and principals at the time that they join the Deloitte U.S. Firms. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of such factors as whether the issues identified are job related or pose a risk to the Deloitte U.S. Firms or to their respective employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining one of the Deloitte U.S. Firms is a partner, principal or employee, and the level of the employee. While background investigations were not always performed on Deloitte U.S. Firms' personnel, and may not always have covered the same information, all background investigations of Deloitte U.S. Firms' personnel in the U.S. currently include the following, at a minimum:

   - SSN verification: confirms a valid number and the names and addresses associated with that number

   - Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:

- Federal courts
- County courts
- State repositories, where the state has made one available and it is reasonably accessible

- A national criminal record database search, including the state sex offender registries
- Education confirmation: all education beyond high school confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

10. Information Security: D&T will comply with its security policies as set forth in Appendix G.

11. Successor/Predecessor Auditor Communication: In the event of a cessation of the client-auditor relationship, we agree to abide by professional standards with respect to communications between predecessor and successor auditors.

12. Dispute Resolution. Any controversy or claim between the parties arising out of or relating to the engagement letter or this engagement (a "Dispute") shall be resolved by mediation or binding arbitration as set forth in the Dispute Resolution Provision attached hereto as Appendix F and made a part hereof; provided, however, to the extent there is an active lawsuit that was initiated by a third party against either Company or D&T ("third party action"), either Company or D&T, as the case may be, may seek resolution of a related Dispute (such as a claim for contribution) against D&T or the applicable Company, as the case may be, in such third party action.

APPENDIX F

DISPUTE RESOLUTION PROVISION

This Appendix F is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

This Dispute Resolution Provision sets forth the dispute resolution process and procedures applicable to the resolution of Disputes and shall apply to the fullest extent of the law, whether in contract, statute, tort (such as *negligence*), or otherwise.

Mediation: All Disputes shall be first submitted to nonbinding confidential mediation by written notice to the parties, and shall be treated as compromise and settlement negotiations under the standards set forth in the Federal Rules of Evidence and all applicable state counterparts, together with any applicable statutes protecting the confidentiality of mediations or settlement discussions. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR"), at the written request of a party, shall designate a mediator.

Arbitration Procedures: If a Dispute has not been resolved within 90 days after the effective date of the written notice beginning the mediation process (or such longer period, if the parties so agree in writing), the mediation shall terminate and the Dispute shall be settled by binding arbitration to be held in San Francisco, California. The arbitration shall be solely between the parties and shall be conducted in accordance with the CPR Rules for Non-Administered Arbitration that are in effect at the time of the commencement of the arbitration, except to the extent modified by this Dispute Resolution Provision (the "Rules").

The arbitration shall be conducted before a panel of three arbitrators. The Companies, on the one hand, and Deloitte & Touche LLP, on the other hand, shall each designate one arbitrator in accordance with the "screened" appointment procedure provided in the Rules, and the two party-designated arbitrators shall jointly select the third in accordance with the Rules. No arbitrator may serve on the panel unless he or she has agreed in writing to enforce the terms of the engagement letter (including its appendices) to which this Dispute Resolution Provision is attached and to abide by the terms of this Dispute Resolution Provision. Except with respect to the interpretation and enforcement of these arbitration procedures (which shall be governed by the Federal Arbitration Act), the arbitrators shall apply the laws of the State of California (without giving effect to its choice of law principles) in connection with the Dispute. The arbitrators shall have no power to award punitive, exemplary or other damages not based on a party's actual damages (and the parties expressly waive their right to receive such damages). The arbitrators may render a summary disposition relative to all or some of the issues, provided that the responding party has had an adequate opportunity to respond to any such application for such disposition. Discovery shall be conducted in accordance with the Rules.

All aspects of the arbitration shall be treated as confidential, as provided in the Rules. Before making any disclosure permitted by the Rules, a party shall give written notice to all other parties and afford such parties a reasonable opportunity to protect their interests. Further, judgment on the arbitrators' award may be entered in any court having jurisdiction.

Costs: Each party shall bear its own costs in both the mediation and the arbitration; however, the parties shall share the fees and expenses of both the mediators and the arbitrators equally.

APPENDIX G

INFORMATION SECURITY STATEMENT

This Appendix G is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and PG&E Corporation and Pacific Gas and Electric Company and acknowledged and agreed to by the Audit Committees of PG&E Corporation and Pacific Gas and Electric Company.

Overview

Deloitte LLP and/or its affiliates ("Deloitte") has developed and implemented an Information Technology ("IT") infrastructure that is designed to generally align with industry standards. The security boundary of the IT infrastructure includes Deloitte-issued laptops, as well as infrastructure and applications, such as databases, document collaboration, email, and backup systems. The IT infrastructure security controls and associated information security processes were developed to protect confidential information while making it available in appropriate circumstances. A summary of such policies, controls, and associated processes is set forth below.

Purpose

The purpose of this Information Security Statement is to provide an overview of Deloitte's IT security practices that are in effect as of the recent published date of this document (4/11/2019). From time to time, Deloitte may modify or update these policies, controls and associated processes. Deloitte shall not be under any obligation to notify any client of any such change to its policies, controls and associated processes.

Cyber Security

Deloitte's Chief Information Security Officer ("CISO") oversees the Cyber Security team, which provides assistance in the following areas:

- eDiscovery Forensic Investigations:
  - Manages the end-to-end process of collecting data requested by the Office of General Counsel ("OGC") for legal and regulatory matters
  - Works with OGC and the Talent organization to conduct internal investigations on misuse of data resources and manages security incident responses
  - Acquires, documents, and preserves digital evidence for computer forensics
- Risk & Compliance:
  - Leads and manages the vendor security program and privacy impact assessment process
  - Collaborates with client service leaders and OGC in responding to client security inquiries and security agreements
  - Leads Deloitte's third party audit and assessment (e.g., SOC2 and Shared Assessments Agreed Upon Procedures)

- Leads Deloitte's security awareness efforts and assists with global security awareness efforts
- Responsible for exceptions to security policies and standards

- Cyber Defense:
  - Monitors, analyzes, and responds to all types of system, device, and application events, such as user activity, firewalls, IDS/IPS, antivirus, and vulnerabilities
  - Identifies, rates, and remediates potential security vulnerabilities of applications and systems
  - Understands which Deloitte systems are used, how, and by whom and uses this information to protect the organization from potential threats

- Data Protection:
  - Reviews emerging technologies, security architecture, and proposals for improvements
  - Leads the identity management program
  - Leads Federal support and maintains FedRAMP certifications
  - Members of the Cyber Security team hold various industry security- and audit-based certifications (e.g., CISSP, CISM, CISA, ISSM, CRISC, CEH, ISO 27001 Lead Auditor, and OSCP)

Information Security Program

Deloitte maintains a comprehensive information security program, which includes policies, standards, procedures and guidelines. The information security program is informed by several industry-standard guidelines and best practices including ISO27001, COBIT, ITIL, American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC2"), and the Shared Assessments Program (formerly known as the "BITS Financial Institution Shared Assessments Program").

Deloitte's IT leadership meets on a regular basis to consider strategic and tactical direction for the information security program, and its policies, standards, procedures and guidelines.

Information security policies are drafted with input from internal information security stakeholders and are based upon industry standard practices. The drafts are reviewed and approved by Deloitte's Cyber Security leadership, OGC, the Office of Confidentiality and Privacy, the CISO and Deloitte's Chief Information Officer. Once approved, the policies are published on Deloitte's intranet and communicated to personnel.

Certification

Deloitte has established and operates an Information Security Management System that manages its client confidential information (ISMS). The ISMS has been certified by an

independent third party that it complies with the requirements of the International Information Security Management System Standard ISO/IEC 27001.

On-Site Security Assessments

In an effort to protect and minimize risk to Deloitte's client data, in lieu of permitting individual clients to perform independent security assessments of Deloitte's information security program, each year Deloitte engages an independent third-party auditor ("Third Party") to (i) conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability established by the AICPA ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC2 Report"), and (ii) apply procedures based upon a version of the Shared Assessments Program Agreed Upon Procedures (the "Shared Assessments AUPs") with respect to certain of Deloitte's information technology controls and to prepare a report with respect thereto (the "Shared Assessments Report").

SOC2 Report

The SOC2 Report includes the Third Party's opinion on the fairness of the presentation of the description of Deloitte's systems in management's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on the Third Party's examination. The SOC2 Report also includes a description of Deloitte's systems and controls, and a description of the Third Party's criteria, test procedures, and the results of such tests. The SOC2 Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the SOC2 Report.

Shared Assessments Report

The Shared Assessments Report is used to assist Deloitte management in evaluating certain IT controls related to the security of Deloitte's client data. The Shared Assessments Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the Shared Assessments Report and has executed an access letter with the Third Party.

The Shared Assessments Program includes the Agreed Upon Procedures (which are a list of security control objectives) and the Standardized Information Gathering ("SIG") questionnaire. Detailed information about the Shared Assessments Program can be found at http://www.sharedassessments.org/. The Shared Assessments Program defines specific controls and objectives as well as the procedures for verifying those controls. The Agreed Upon Procedures address the following controls areas:

- Risk management
- Information security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management

- Business continuity management
- Compliance
- Privacy

Awareness and Training

Deloitte has implemented training and awareness programs for its personnel related to information-security, confidentiality and privacy policies and practices. Deloitte personnel are required to complete a confidentiality, privacy, and information security awareness training during the new-hire onboarding process, as well as an annual update course thereafter. Deloitte personnel are presented with an information security policy awareness statement via Deloitte's intranet two times each year, which they are required to acknowledge within two weeks of the statement's release.

Deloitte has a dedicated security awareness committee. The committee is responsible for developing ideas to enhance Deloitte's awareness of security risks and issues through policy development and training. The committee is comprised of delegates from Deloitte's Cyber Security leadership, National Office of Security, Office of Confidentiality and Privacy, CISO, National Quality Risk Management, Talent, and OGC, and from Deloitte Touche Tohmatsu Limited's Global Information Security Office, who regularly meet to discuss new or recurring security issues, devise strategies and implementation plans, and provide progress reports on existing projects.

Management and Protection of Confidential Information

Deloitte is committed to protecting the confidential information, including Personally Identifiable Information (PII), of our clients, our organization and the third parties with whom we work. "Confidential Information" refers to any information not generally available to the public, in any form, that Deloitte receives or creates in the course of business. To support this commitment, Deloitte has established the Office of Confidentiality and Privacy which is responsible for setting guidelines, developing procedures, and providing consultation and training on the management of Confidential Information.

The Office of Confidentiality & Privacy has also developed the "Confidential Information Program" for the proactive management and protection of Confidential Information and is responsible for implementing the Confidential Information Program across Deloitte. The Confidential Information Program consists of processes, technology controls, training, and communications that help our professionals to improve their awareness of risks associated with Confidential Information and their ability to properly manage and safeguard Confidential Information.

The Confidential Information Program

The Confidential Information Program consists of processes and activities that are performed throughout the engagement lifecycle to manage and protect Confidential Information.

Client account and engagement teams in the Confidential Information Program generally do the following:

- Appoint a data manager responsible for overseeing program activities;
- Develop and maintain a Confidential Information management plan to document the Confidential Information management strategy and safeguards employed;

- Develop and deliver Confidential Information onboarding training that outlines the protocols that team members must follow when accessing, storing, using, transferring, and disposing of Confidential Information;

- Implement physical, administrative, and technical safeguards identified in the Confidential Information management plan to proactively manage risk; and

- Complete all other required confidentiality training as applicable.

Deloitte also has an insider threat program in which Deloitte conducts active monitoring of insider threats. Insiders are defined as personnel and contractors who, based on their access to certain systems and information, could adversely affect the brand, reputation and/or business of Deloitte or its clients. Leveraging potential risk indicators, the insider threat program monitors persons of interest across a broad risk spectrum, including workplace violence, espionage, fraud, and theft of intellectual property and Confidential Information. Analytic and cognitive technologies are used to help identify indicators of poor risk-culture fit and determine corresponding strategic tactics and mitigation strategies to align our sub-cultures.

Data Privacy

Deloitte is committed to protecting our clients' Personally Identifiable Information ("PII"). Deloitte has a data privacy policy, applicable procedures, and personnel dedicated to making sure we comply with applicable data privacy laws and regulations. We regularly monitor for changes in data privacy laws and regulations and adjust our policies and procedures when appropriate. Additionally, we have instituted an annual review process across all Deloitte business areas to verify compliance with our privacy policy and procedures.

- Deloitte has policies and procedures that protect PII and support compliance with US and the European Union (EU) legal requirements relating to the transfer and processing of PII, including personal health information.

- Deloitte adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to PII that is transferred from the European Economic Area and Switzerland to the United States.

- Deloitte is not a "Covered Entity" as defined under the Health Insurance Portability and Accountability Act, as amended ("HIPAA"). Therefore, Deloitte is generally not required to, and does not, comply with the obligations of a Covered Entity. However, when Deloitte acts in the capacity of a "Business Associate" to our clients, as such role is defined under HIPAA, Deloitte is required to comply with the obligations of a Business Associate under HIPAA. Deloitte has implemented policies, procedures, and controls that facilitate compliance with those obligations.

- Deloitte utilizes a Privacy Impact Assessment (PIA) process for new systems, changes to existing systems and high-risk business processes that access, transfer or store PII.

- In support of the Privacy by Design concept, Deloitte has incorporated privacy and confidentiality requirements into our secure systems development lifecycle (SSDLC) for internally developed systems so that these requirements are

considered early and often throughout the lifecycles of technology projects using a risk-based approach.

Confidentiality and Privacy Incident Management

Deloitte has instituted an integrated incident response process designed to facilitate prompt reporting and resolution of incidents. Our confidentiality and privacy incident response process is characterized by the following:

- Centralized reporting of actual or suspected incidents to a Help Desk, which is available 24/7 with access via a toll-free number;
- Training and awareness programs focused on helping personnel understand immediate steps to be taken in case of actual or suspected incidents;
- Established roles and responsibilities for incident management and response including involving the appropriate consultation resources across the Deloitte organization, as applicable to the specific matter;
- Documented processes to help gather incident facts, initiate response activities, engage incident response teams, escalate incidents and alert appropriate leaders, based on the nature of the specific incident;
- Consultation among the relevant parties regarding the need for a corrective action plan;
- Development, as appropriate, of action plans, including any required communications, as well as actions to mitigate the risk of a future recurrence; and
- Post-incident follow-up process to analyze root causes and integrate lessons learned.

IT Continuity Management

Deloitte maintains an active disaster recovery and business continuity program which helps to continue delivering information-technology-related services should a disruption occur. Deloitte's program includes the following basic activities:

- Business continuity planning for IT infrastructure support staff;
- Business impact assessments to help define criticality of processes and systems related to recovery time objectives;
- Disaster recovery planning of our technology through multiple failover capabilities;
- Implementation of resilient architectures where technology allows;
- Risk assessments as part of continual service improvement, with countermeasures identified and implemented for the newest scenarios; and
- Internal review process for maintaining the quality of plans and services.

The business continuity program ("BCP") and plans include emergency-response business procedures, which go into effect following the occurrence of a disaster or other unplanned interruption.

Disaster recovery ("DR") plans include technical and business contact call lists, as well as notification and escalation information and architecture diagrams. Where pertinent, third-party information is also included. Recovery time objectives and recovery point objectives are documented and tested for each plan.

BCP/DR plans for critical infrastructure are subject to review and testing every 12 months with industry standard testing methods.

Risk assessment test scenarios vary based on business sensing and technology security. Test results are reviewed and recorded.

In summary, Deloitte has a comprehensive disaster recovery and business continuity program that is designed to provide for the continuity of essential IT business functions and critical business processes following the occurrence of a disaster or other unplanned interruption impacting Deloitte's IT infrastructure.

Business Continuity Management

Deloitte takes disaster and contingency planning very seriously, including planning for events that impact its people and/or its facilities. Deloitte's business continuity planning addresses issues such as, communications, travel, resource allocation, technology needs, and alternate work sites. Response procedures assess the well- being of personnel, provide for the continuity of essential business functions, and utilize recovery procedures for the restoration of critical business processes. Cross-functional teams are identified to manage potential disruptive events, emergency situations or disasters. Each Deloitte office has a local crisis management team to handle smaller, localized events impacting a single location. For larger events or those that are not specific to a single location or geography, an experienced national incident support team is assigned ("National Incident Support Team"). A national crisis council handles incidents that rise to the level of a true crisis requiring strategic involvement and decision-making.

Cross-functional teams are identified and documented in the plans to include representation of key stakeholders from the following areas:

- Client Services
- Office Services/Operations/Facilities
- Office of Security
- Human Resources and Benefits
- Information Technology Services
- Procurement and travel
- Communications
- Risk Management

Deloitte has designed an impact-driven approach, which focuses on the impacts of an event, emergency, or crisis, rather than specific scenarios. Each type of situation could have an impact on our people, our facilities, our technology, or our clients. Each type of situation could require communications, whether internal or external. The team-based, impact-driven approach utilized by Deloitte provides the best resources to assess and address the impacts of an event.

Deloitte has developed a specific plan to address the impacts and continuity of operations in light of a pandemic ("Pandemic Plan"). The Pandemic Plan and related governance model is aligned with the crisis management and business continuity processes, including the use of the National Incident Support Team, but is supplemented by additional members of a Pandemic Response Committee. The Pandemic Response Committee monitors potential pandemic developments and would oversee implementation of specific pandemic action steps based on the severity of the pandemic, including targeted communications that would be issued internally and externally, and identification of critical people and resources.

Limits of Business Continuity and Pandemic Planning

Due to the significant uncertainties associated with a possible flu pandemic or other disaster, Deloitte can make no representations or warranties, nor provide any assurances, that its plans will be adequate to respond to any possible consequences, or that the plans of any third parties to deal with a possible flu pandemic or other disaster are or will be sufficient to address any situations or problems that might arise during a pandemic or other disaster. Deloitte's objective is to prepare for a possible flu pandemic or other disaster based on the information and data that it has at this time, and to possibly modify those plans as it believes conditions or facts may warrant. Every organization needs to develop its own preparedness plan based on its specific circumstances, business functions, and operational factors. Consequently, a plan developed for one function or business cannot be expected to address the potential issues that may be faced by another business enterprise. Because business continuity and disaster recovery plans and documentation contain information about Deloitte that is proprietary and confidential, Deloitte does not provide third parties with copies of such plans or documentation.

Human Resources Security

Upon hire, all personnel agree to comply with Deloitte's policies, including those relating to information security, confidentiality and privacy. In addition, all Deloitte personnel are required to complete security awareness training during the new hire onboarding process.

Background Checks for U.S. Personnel

Deloitte generally requires that background investigations be conducted for partners, principals and all employees at the time that they join Deloitte. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of whether the issues identified are job-related or pose a risk to Deloitte or to its employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining is a partner or principal and the level of the employee. While background investigations were not always performed on Deloitte personnel, and may not always have covered the same information, all background investigations of Deloitte personnel in the U.S. currently include the following, at a minimum:

- SSN verification: confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:
    - Federal courts
    - County courts
    - State repositories, where the state has made one available and it is reasonably accessible

- A national criminal record database search, including the state sex offender registries.
- Education confirmation: education beyond high school confirmed
- Employment confirmation: professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

Background checks for Personnel of Deloitte entities located in India ("U.S. India")

The type of background investigation performed depends on whether the individual joining U.S. India is a partner, principal, or employee, and the level of the employee. While background investigations were not always performed on U.S. India's personnel and may not always have covered the same information, all background investigations of U.S. India personnel currently include the following, at a minimum:

- Identity Verification, where possible
- Criminal checks: check all relevant court records for a five year period
- Education confirmation: all university level education is confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, including India specific and global databases
- Professional licenses: confirm relevant professional licenses

Physical and Environmental Security

Only authorized personnel with a Deloitte-issued electronic badge are granted access to Deloitte's facilities. Procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the facilities. Deloitte data centers are further restricted to only those personnel with the need to access restricted areas. Data centers have the following physical security measures: security guards, man-trap doors at primary entrance, multi-factor authentication (Deloitte-issued electronic badge and biometric readers) at secondary entrance, video cameras, and sign-in and sign-out sheets for escorted visitors.

The electricity, water, and temperature controls are all pre-approved for use by the facilities administrators in the data centers. Each utility has a control in place to monitor its usage and to notify an administrator in case of failure. Automatic emergency lighting is installed in areas necessary to maintain personnel safety.

Emergency exits are located in appropriate places in Deloitte facilities. Automatic fire suppression systems have been installed to protect the facilities. In data centers, the primary system is HFC-125 chemical based and activated via multiple smoke detectors, and the second type is pre-action hydronic, and the detection method is temperature. Master water shut-off valves are present. Temperature and humidity controls have been implemented to protect against temperature fluctuations in all areas of the data centers containing IT equipment.

Risk Management

Deloitte has a risk management program that monitors possible threats and

vulnerabilities to information technology assets. Risk assessment(s) are performed annually and when there are significant changes to infrastructure, technology or environment. There are several control domains defined for risk assessment. These control domains are derived from industry standard practices and frameworks. For each control domain, implemented controls are identified and tailored and their effectiveness assessed for risk management. Risks that are not at an acceptable level are remediated or mitigated.

Vendor Hosting and Processing

Deloitte has arrangements with vendors who provide Deloitte with certain software-as-a service and hosting services. Deloitte selects and retains these vendors based on, among other qualities, their capability to maintain safeguards for the systems, software and information at issue that are consistent with leading industry security practices. Deloitte requires these vendors to implement and maintain such safeguards.

Vendor Assessment Process

The Vendor Assessment process is designed to reduce vendor-related risk by:

- Building a repository of acceptable vendors;
- Assessing the security posture of vendors;
- Tracking remediation of identified issues; and
- Reviewing and assisting with vendor contracts with respect to obligations relating to Deloitte's information security program.

Asset Management

Deloitte has an asset management team that is responsible for oversight and management of Deloitte assets and inventory throughout its lifecycle. There are tools and controls in place that manage hardware and software assets. Deloitte has policies and procedures in place to manage licensed software and security controls to deter prohibited software from being installed and/or used. A software and hardware inventory system is maintained, which identifies hardware and software components used within Deloitte information systems. Multiple controls are used to manage the configuration baselines, including mobile device management. These controls are supported by automated tools that provide configuration and inventory information on a continuous basis specific to configuration compliance, known vulnerabilities, inventory by Internet Protocol address ("IP address")/device name and asset operational and connection status.

Access Control

Access to Deloitte information contained on Deloitte IT systems is granted on a need-to-know basis and must be approved by the Deloitte data owner.

Vendor and contractor access is requested through procedures that involve Deloitte's Talent and Technology groups. Upon approval, the vendor user accounts are created in a controlled domain organizational unit giving the access necessary to perform their defined duties. Vendor and contractor access is granted on a temporary basis based on business need.

For certain systems, remote access is provided via a Secure Sockets Layer ("SSL") Virtual Private Network ("VPN") using two-factor authentication with account activity being logged to Deloitte's logging/alerting mechanism. Depending on the level and type of access

required, the SSL VPN solution provides a virtual session or web interface with access into the needed application(s) or platform.

For web-based applications that contain or provide access to sensitive internal or client data (including VPN), Multi-Factor Authentication (MFA) has been enabled. Verification options include phone call, text message, or mobile application.

Privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into role-based groups (e.g., key management, network, system administration, database administration, and web administration).

Identification and Authentication

All users must authenticate to the Deloitte network using a unique user identification ("ID") and a strong password prior to gaining access to the information system.

Deloitte strong passwords contain the following characteristics:

- Passwords are required to be at least ten (10) characters in length and contain at least three of the following four elements: (1) westernized Arabic numbers (e.g., 2,5,9), (2) non- alphanumeric characters (e.g., #, %, !, %, @, ?, -, *), (3) English uppercase letters (e.g., A, B, C), and/or (4) English lowercase letters (e.g., a, b, c)
  - Passwords are not permitted to contain:
    - parts of the users' username, first name, or last name
    - dictionary words with or without (i) numbers or special characters at the beginning or end, or (ii) letters, numbers, or character exchanges (e.g., Summer2017, ?Happyman, H3llofr!end?)
    - words or numbers connected with users such as family names, petnames, birthdays, addresses, or phone numbers
    - common terminology, acronyms, or names associated with the Deloitte or its clients
    - any variation of 'Deloitte' or 'Password' (e.g., Deloitte12, P@ssw0rd12, Pa$$w0rd!2)
    - any sequencing of letters and numbers that follow the order of a keyboard (i.e., keyboard walk patterns such as 1234qwerASDF, 1qazXSW@3edc)

Additional Password Safeguards

The following additional password related safeguards are enforced:

- Users are not permitted to reuse their previous twenty-four passwords
- Passwords expire every 90 days
- There is a password lockout threshold after 6 invalid logon attempts

System Security

System and Communications Protection

An intrusion prevention system ("IPS") is employed at the point of entry to the Deloitte network environment. The logs for the IPS, firewall, and VPN are sent to a log aggregator. Access control lists are placed on firewalls controlling the inbound and outbound flow of traffic. Traffic is denied by default unless approved by the gateway protocols as configured and approved by the Deloitte security team. A demilitarized zone ("DMZ") and trusted zones are used to segment traffic to areas that are protected in accordance with the accepted risk levels.

System and Information Integrity

Firewall, IPS, and VPN audit logs are sent to the log aggregator, which checks for abnormal activity and anomalous behavior that would trigger an information security review. Hardware and software checks are done by automated tools with identified alert levels that trigger a notification to the system administrators in case of a system flaw. Anti-virus and malware protection is managed by enterprise policy and distributed by a server located in the environment periodically. Anti-virus is configured to scan external devices attached to the information system as well as email traffic.

Data Back-up

Deloitte systems are scheduled for daily backup and two iterations of data through redundant data mirroring: one onsite and one offsite. If a system backup is interrupted for any reason, it will resume on the alternate site where it left off. A reputable vendor is utilized for offsite backup storage and disposal. All backup media is encrypted prior to shipment to the vendor and a controlled process exists for turnover. The vendor is subject to obligations of confidentiality. The vendor has security practices in place and uses a tracking application for all media it handles on Deloitte's behalf. Deloitte is provided with inventory reports of the media and chain-of-custody. The vendor stores the media in a secure, environmentally-controlled storage facility.

Information Systems Acquisition, Development and Maintenance

Security Planning

The Deloitte information security program, applicable policies, standards, standard operating procedures and guidelines are reviewed annually and updated as necessary.

Acquisition of System and Services

Deloitte does not acquire IT systems or services until Cyber Security has reviewed the product or service to determine whether it meets internal guidelines with respect to security and encryption. Software installation requests are submitted for risk assessment and approval. Software is not implemented unless it meets applicable Information Technology Services ("ITS") standards. There is a Change Control Board ("CCB") that discusses any changes that may affect the security posture of the environment and documents all proposed upgrades or modifications to the environment, assets and infrastructure.

Application Development

Deloitte follows secure coding best practices during the system development lifecycle for

Deloitte applications. Deloitte's applications undergo security reviews, testing and vulnerability scans prior to being placed in production.

Change Control

Deloitte has a change management process in place for its IT systems. Proposed changes are submitted, tested, and reviewed during regularly scheduled CCB meetings. Approved changes are tested and vulnerability scans are performed prior to deployment. Deployment windows are scheduled to minimize the impact to Deloitte's operations. Back-out plans are in place should they be needed.

Patch Management

Deloitte has a patch-management program and supporting tools in place that are managed by an internal patch management team ("PMT"). Vendor and industry-accepted alert lists are monitored for new patches. Patches are reviewed by the PMT at regularly scheduled meetings and are rated for deployment based on assessed severity levels. Emergency patch management meetings are called when needed.

Vulnerability Management

Deloitte's network undergoes penetration testing and vulnerability scans performed by Deloitte's Cyber Defense team. Penetration tests are performed annually on the network infrastructure's external perimeter by Deloitte's Cyber Defense team. Vulnerability scanning is performed weekly on the network infrastructure's internal and external perimeter by Deloitte's Cyber Defense team.

Maintenance

Deloitte ITS performs software and hardware maintenance on Deloitte's environment servers.

Information system backups are performed daily. Performance reports are initiated through automated tools that specify certain levels of performance to trigger the generation of the report (i.e., % of CPU processor utilization, etc.).

Third-party contractor maintenance personnel must be approved prior to receiving access to the information system servers. Third party maintenance personnel are escorted into the facility and accompanied during the period of access. A log is maintained which documents the name, date, length of time, justification, and escort name for each maintenance individual who is granted access to the information system(s).

Information Security Incident Management

Deloitte has built an integrated incident response team that brings together the appropriate subject matter experts from various cross-functional disciplines to address each specific incident. The Security Incident Response Procedures ("Procedures") describe how various types of incidents are handled. The Procedures identify key resources and communications that will take place based on various incident types. The Procedures identify to whom suspected incidents should be reported and describe the escalation path from the entry point in the process through fruition. Security awareness training is in place to educate Deloitte personnel of their responsibilities concerning security incidents. Each incident is logged, and the relevant facts are captured for analysis and reporting. When necessary, data related to the incident is maintained in a forensically sound manner and appropriate chain-of-custody is documented.

The incident response team has a variety of tools available to assist them in the analysis of incidents. These include standard security tools from software and hardware providers as well as commercial forensic tools specifically targeted for such matters.

Information security incident procedures are executed periodically so the teams remain prepared for response should the need arise. At the completion of each significant incident, a post-incident review is conducted to identify any areas for improvement as well as lessons learned. These findings are used to adjust, enhance or improve the procedures.

Compliance

System Audit and Accountability

System audit logs and records are created to monitor the following

- anti-virus services
- intrusion prevention services
- remote access services, web proxy services
- domain authentication
- router events
- firewall events
- VPN access
- application logs
- operating system logs
- privileged access logs

System audit logs are maintained to support analyses and investigations. Logs are maintained for a period of one (1) year. Logs may also be preserved based on legal or regulatory requirements.

System audit log content includes: (i) date and time of the security event; (ii) the component of the information system (e.g., software component, hardware component) where the security event occurred; (iii) type of security event; (iv) unique user/subject identity; and (v) the outcome (success or failure) of the security event.

System Audits

Deloitte's internal audit team periodically performs internal audits on various aspects of Deloitte's systems, processes, and policies.

Application Configuration Management

Software baseline requirements are created in accordance with Deloitte policies and standards. Software is tested against the baseline requirements prior to being placed in the production environment. Continued monitoring and change management processes are conducted while in operation.

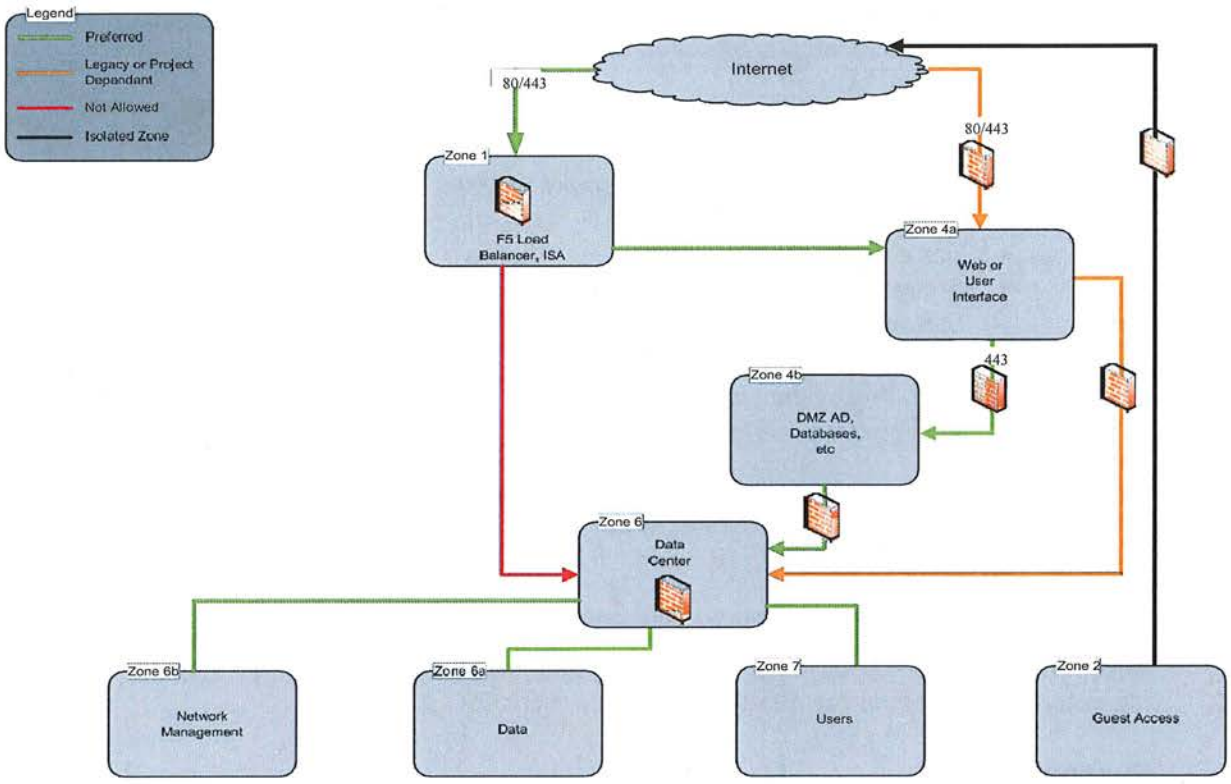
Wireless Access

Deloitte supports an internal wireless network within the organization. A wireless-security and acceptable- use policy is in place. Only Deloitte-approved access points will be connected to Deloitte's network.

- For wireless access to Deloitte's networks, personnel are required to use Wi-Fi Protected Access (WPA2 or stronger protection) where it is available.
- For the convenience of visitors, clients, or guests, a guest wireless network providing controlled access to the Internet may be made available in Deloitte's facilities.

Data Flow Diagram

Zone Flow – Basic Rules for Zone Flow



Data Protection

Deloitte personnel receive training on the proper handling of PII. In instances where Deloitte may transmit client PII outside of the Deloitte environment, Deloitte requires transmission of such data in an encrypted format.

Media Protection

Secure printing is available at multiple locations within each Deloitte office that requires the usage of a Deloitte-issued electronic smartcard badge to enable the print job. Further, Deloitte issues encrypted USB drives to its personnel that meet the encryption standards outlined in Federal Information Processing Standard ("FIPS") 140-2. In addition, software has been deployed to Deloitte-issued IT assets as part of the standard application toolset that allows the creation of encrypted WinZip files (FIPS 197 compliant).

Deloitte has implemented a technical control that encrypts data written/copied to external USB devices which can only be read by a Deloitte machine.

Laptops are encrypted and are required to be physically secured at all times. Physical access to servers is restricted to authorized parties. Magnetic drives are wiped/over-written with a minimum of three passes with a media sanitization tool prior to being released for re-use and disposal.

Deloitte has employed the following methods of PDA protection: 1) forced access PINs; 2) remote wipe in the event of 10 incorrect pin attempts; 3) remote wipe if the PDA is reported as lost or stolen; 4) encryption; and 5) an installed mobile device management tool.

Data Destruction

Policies and practices are in place with regard to the destruction of confidential information and PII that vary depending on type of media on which such information is stored. Deloitte is aligned with the National Institute for Standards and Technology's ("NIST") guidelines for media sanitization. For example, hard disks, CD/DVD, USB drives are required to be wiped using a disk cleaning tool, while tapes are required to be destroyed at end-of-life. Paper containing such information is required to be shredded.

Encryption

Whole-disk encryption has been deployed on Deloitte-issued laptops. Deloitte's laptops have deployed encryption with the 256-bit Advanced Encryption Standard ("AES") algorithm.

Deloitte has deployed encrypted USB drives intended for use in transporting sensitive or confidential data. This encryption method is FIPS 140-2 compliant.

WinZip is installed on all Deloitte-issued laptops. This encryption method is FIPS 197 compliant.

Additionally, Deloitte Internet email gateways are configured to attempt to transmit all email in an encrypted manner, using opportunistic TLS encryption, if the recipient of the transmission can support such encryption methodology. If TLS is enabled on the recipient email gateway, the email will be encrypted between the Deloitte gateway and the recipient gateway. TLS encryption can also be enforced when agreed with the recipient organization. This encryption method is FIPS 140-2 compliant.

Data in transit is protected by secure TLS using certificates with minimum 2048-bit RSA key and SHA2 signing when using Deloitte secure websites and file transfer services.

Secure File Transfer Protocol ("SFTP") is an available option for the transfer of client data. SFTP securely encrypts and compresses files during transmission. This encryption method is FIPS 140-2 compliant.

Records Management

Deloitte maintains and retains records in accordance with applicable legal and regulatory requirements and professional standards. Specific areas of focus include:

- Facilitating compliance with external requirements and internal policies and practices pertaining to record retention;
- Managing recordkeeping critical to the operation of our business and service to our clients;
- Designing and implementing records management technology, tools, and standard processes;
- Coordinating the proper handling of files on legal hold due to legal, tax or regulatory preservation requirements; and
- Maintaining a strong, compliance-focused records and information management governance organization.

Deloitte.

Deloitte & Touche LLP
555 Mission Street
Suite 1400
San Francisco, CA 94105
USA

Tel:+1 415 783 4000
www.deloitte.com

December 10, 2019

Mr. Nicholas M. Bijur
Chairman
The Nuclear Facilities Decommissioning Master Trust Committee
77 Beale Street
San Francisco, CA 94105

Mr. David S. Thomason
Vice President, Controller, and Chief Financial Officer
Pacific Gas and Electric Company
77 Beale Street
San Francisco, CA 94105

Dear Mr. Bijur and Mr. Thomason:

Deloitte & Touche LLP ("D&T" or "we" or "us") is pleased to serve as independent auditors for the Nuclear Facilities Non-Qualified CPUC Decommissioning Master Trust, the Nuclear Facilities Qualified CPUC Decommissioning Master Trust, and the Nuclear Facilities Qualified FERC Decommissioning Master Trust (individually, the "Trust"; collectively the "Trusts") of Pacific Gas and Electric Company (the "Company" or "you" or "your"). Mr. Timothy Gillam will be responsible for the services that we perform for the Trusts hereunder.

In addition to the audit services we are engaged to provide under this engagement letter, we would also be pleased to assist the Company on issues as they arise throughout the year. Hence, we hope that you will call Mr. Gillam whenever you believe D&T can be of assistance. This assistance will require approval by as applicable, the Nuclear Facilities Decommissioning Master Trust Committee (the "Trust Committee"), and the Company's Audit Committee of the Board of Directors ("the Audit Committee"), in accordance with its preapproval policies and procedures.

The services to be performed by D&T pursuant to this engagement are subject to the terms and conditions set forth herein and in the accompanying appendices. Such terms and conditions shall be effective as of the date of the commencement of such services.

Audits of Financial Statements

Our engagement is to perform audits in accordance with auditing standards generally accepted in the United States of America ("generally accepted auditing standards"). The objective of an audit conducted in accordance with generally accepted auditing standards is to express opinions on whether each of the Trusts' financial statements for the year ending December 31, 2019, are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America ("generally accepted accounting principles").

Appendix A contains a description of the auditor's responsibilities and the scope of an audit in accordance with generally accepted auditing standards.

D&T Reports

We expect to issue written reports upon the completion of our audits. Our ability to express any opinion or to issue any report as a result of this engagement and the wording thereof will, of course, be dependent on the facts and circumstances at the date of our reports. If, for any reason, we are unable to complete any of our audits or are unable to form or have not formed any opinion, we may decline to express any opinion or decline to issue any report as a result of this engagement. If we are unable to complete any of our audits, or if any report to be issued by D&T as a result of this

engagement requires modification, the reasons for this will be discussed with the Trust Committee and the Company's management.

Management's Responsibilities

Appendix B describes management's responsibilities.

Responsibilities of the Audit Committee and the Trust Committee

As independent auditors of the Trusts, we acknowledge that the Trust Committee is directly responsible for the appointment, compensation, and oversight of our work, and accordingly, except as otherwise specifically noted, we will report directly to the Trust Committee. You have advised us that the services to be performed under this engagement letter, including, where applicable, the use by D&T of affiliates or related entities as subcontractors in connection with this engagement, has been approved by the Trust Committee and approved by the Audit Committee in accordance with the Audit Committee's established preapproval policies and procedures.

Communications with the Trust Committee

Appendix C describes various matters that we are required by generally accepted auditing standards to communicate with the Trust Committee and management.

Fees

We estimate that our fees for this engagement will be $75,000. Based on the anticipated timing of the work, our fees will be billed monthly.

Subject to any applicable Bankruptcy Court (as defined below) order, rules or procedures, and payments are due 45 days from the date of the invoice. Engagement-related expenses, and technology- and administrative-related charges will be billed in addition to the fees and will be stated separately on the invoices.

Our continued service on this engagement is dependent upon payment of our invoices in accordance with these terms. Our estimated fees are based on certain assumptions, including (1) timely and accurate completion of the requested entity participation schedules and additional supporting information, (2) no inefficiencies during the audit process or changes in scope caused by events that are beyond our control, (3) the effectiveness of internal control over financial reporting throughout the period under audits, (4) a minimal level of audit adjustments (recorded or unrecorded), and (5) no changes to the timing or extent of our work plans. We will notify you promptly of any circumstances we encounter that could significantly affect our estimate and discuss with you any additional fees, as necessary.

Chapter 11 Proceeding

With respect to services performed prior to the date of each Company's emergence from its Chapter 11 proceeding, D&T expects to apply for compensation for professional services rendered and for reimbursement of expenses incurred, in accordance with applicable provisions of title 11 of the United States Code (the "Bankruptcy Code"), the Federal Rules of Bankruptcy Procedure, the applicable local rules of bankruptcy procedure (the "Local Rules"), the United States Bankruptcy Court Northern District of California Guidelines for Compensation and Expense Reimbursement of Professionals and Trustees, effective February 19, 2014, and the United States Trustee Guidelines for Reviewing Applications for Compensation and Reimbursement of Expenses Filed under Bankruptcy Code § 330 (collectively, the "Fee Guidelines", and any further orders of the Bankruptcy Court regarding the payment of fees and reimbursement of expenses of professionals (the "Orders"). In such event, payment of fees and reimbursement of expenses will be subject to ultimate allowance and approval by the Bankruptcy Court. However, in the interim, each Company will ask the Bankruptcy Court for

approval to allow D&T to submit invoices to each Company for prompt payment in accordance with the Local Rules, the Fee Guidelines, and the Orders. If applicable, payment of these invoices will be made by each Company on an interim basis subject to approval and allowance upon application to and order by the Bankruptcy Court.

Each Company agrees that it will promptly seek the Bankruptcy Court's approval of this engagement and the Engagement Letter. The application, proposed order and other supporting documents (collectively, the "Application") submitted to the Bankruptcy Court seeking its approval of this engagement must be reasonably satisfactory to D&T in all respects. In addition to D&T's other rights or remedies hereunder, D&T may, in its sole discretion and without any liability arising there from, terminate this engagement in the event that (a) a third party files a formal written objection with the Bankruptcy Court to D&T's retention by each Company on the terms and conditions set forth in this Engagement Letter, (b) a final order authorizing the employment of D&T is not issued by the Bankruptcy Court on or before thirty (30) days from the filing date of the Application, or (c) the Application is denied by the Bankruptcy Court; provided that, in the case of (a) or (b), D&T provides each Company and the Trusts with three (3) days' written notice prior to terminating this engagement as a result of any of the aforementioned events. In any such event, each Company hereby agrees to withdraw or amend, promptly upon D&T's request, any Application filed or to be filed with the Bankruptcy Court to retain D&T's services in the Chapter 11 proceeding.

For purposes of this Engagement Letter, together with the General Business Terms and Appendix E attached hereto, "Bankruptcy Court" shall mean the United States Bankruptcy Court with which each Company has filed a Chapter 11 petition.

Inclusion of D&T Reports or References to D&T in Other Documents or Electronic Sites

If the Company or the Trusts intend to publish or otherwise reproduce in any document any report issued as a result of this engagement, or otherwise make reference to D&T in a document that contains other information in addition to the audited financial statements (e.g., in a periodic filing with a regulator, in a debt or equity offering circular, or in a private placement memorandum), thereby associating D&T with such document, the Company and the Trusts agree that the Company's management will provide D&T with a draft of the document to read and obtain our approval for the inclusion or incorporation by reference of any of our reports, or the reference to D&T, in such document before the document is printed and distributed. The inclusion or incorporation by reference of any of our reports in any such document would constitute the reissuance of such reports. The Company and the Trusts also agree that the Company's management will notify us and obtain our approval prior to including any of our reports on an electronic site.

Our engagement to perform the services described herein does not constitute our agreement to be associated with any such documents published or reproduced by or on behalf of the Company or the Trusts. Any request by the Company or the Trusts to reissue any report issued as a result of this engagement, to consent to any such report's inclusion or incorporation by reference in an offering or other document, or to agree to any such report's inclusion on an electronic site will be considered based on the facts and circumstances existing at the time of such request. The estimated fees outlined herein do not include any procedures that would need to be performed in connection with any such request. Should D&T agree to perform such procedures, fees for such procedures would be subject to the mutual agreement of the Company or the Trusts and D&T.

* * * * *

The parties acknowledge and agree that D&T is being engaged under this engagement letter to provide only the services described herein. Should the Company, the Trusts, or the Trust Committee request, and should D&T agree to provide, services (including audit services) beyond those described herein, such services will constitute a separate engagement and will be governed by a separate engagement letter.

This engagement letter, including Appendices A through F attached hereto and made a part hereof,

constitutes the entire agreement between the parties with respect to this engagement and supersedes any other prior or contemporaneous agreements or understandings between the parties, whether written or oral, relating to this engagement.

If the above terms are acceptable and the services described are in accordance with your understanding, please sign the copy of this engagement letter in the space provided and return it to us.

Yours truly,

Deloitte & Touche LLP

Accepted and agreed to by Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts (Nuclear Facilities Decommissioning Master Trust Committee confirms that it has the power and authority to execute this engagement letter, including the appendices attached hereto, on behalf of, and to bind, the Trusts):

By: _____

Title: Vice President Treasurer

Date: 1/17/20

Accepted and agreed to by
Pacific Gas and Electric Company:

By: _____

Title: Vice President & Controller, Utility CFO

Date: 1/14/20

cc: the Audit Committee of the Board of Directors of Pacific Gas and Electric Company

APPENDIX A

AUDITOR'S RESPONSIBILITIES AND SCOPE OF AN AUDIT IN ACCORDANCE WITH GENERALLY ACCEPTED AUDITING STANDARDS

This Appendix A is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and the Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts, and Pacific Gas and Electric Company.

Auditor's Responsibilities

Our responsibilities under generally accepted auditing standards include forming and expressing an opinion about whether the financial statements that have been prepared by management with the oversight of the Trust Committee are presented fairly, in all material respects, in accordance with generally accepted accounting principles. The audits of the financial statements do not relieve management or the Trust Committee of their responsibilities.

Scope of an Audit

Generally accepted auditing standards require that we plan and perform the audits to obtain reasonable, rather than absolute, assurance about whether the financial statements as a whole are free from material misstatement, whether caused by fraud or error. However, because of the inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk exists that some material misstatements may not be detected, even though the audits are properly planned and performed in accordance with generally accepted auditing standards. We have no responsibility to plan and perform the audits to obtain reasonable assurance that misstatements, whether caused by fraud or error, that are not material to the financial statements as a whole are detected.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on our judgment, including the assessment of the risks of material misstatement of the financial statements, whether caused by fraud or error. In making those risk assessments, we consider internal control relevant to the Trusts' preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances but not for the purpose of expressing an opinion on the effectiveness of the Trusts' internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

APPENDIX B

MANAGEMENT'S RESPONSIBILITIES

This Appendix B is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and the Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts, and Pacific Gas and Electric Company.

Financial Statements

Management is responsible for the preparation, fair presentation, and overall accuracy of the financial statements in accordance with generally accepted accounting principles. In this regard, management has the responsibility for, among other things:

- Selecting and applying the accounting policies
- Designing, implementing, and maintaining effective internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error
- Identifying and ensuring that the Trusts comply with the laws and regulations applicable to their activities and informing us of all instances of identified or suspected noncompliance with such laws or regulations
- Providing us with (1) access to all information of which management is aware that is relevant to the preparation and fair presentation of the financial statements, such as records, documentation, and other matters, (2) additional information that we may request from management for the purpose of our audits, and (3) unrestricted access to personnel within the Company from whom we determine it necessary to obtain audit evidence

Management's Representations

We will make specific inquiries of the Company's management about the representations embodied in the financial statements. In addition, we will request that management provide us with the written representations the Trusts are required to provide to their independent auditors under generally accepted auditing standards. The responses to those inquiries and the written representations of management are part of the evidential matter that D&T will rely on in forming its opinion on the Trusts' financial statements. Because of the importance of management's representations, the Company and the Trusts agree to release and indemnify D&T, its subcontractors, and their respective personnel from all claims, liabilities, and expenses relating to our services under this engagement letter attributable to any misrepresentation by management.

Process for Obtaining Preapproval of Services

Management is responsible for the coordination of obtaining the preapproval of the Audit Committee, in accordance with the Audit Committee's preapproval process, for any services to be provided by D&T to the Trusts.

Independence Matters

In connection with our engagement, D&T, management, and the Audit Committee will assume certain roles and responsibilities in an effort to assist D&T in maintaining independence and ensuring compliance with the securities laws and regulations with respect to D&T's role as the Company's independent auditor. D&T will communicate to its partners, principals, and employees that the Trusts are attest clients. Management of the Company will ensure that there are policies and procedures in

place for the purpose of ensuring that neither the Trusts, the Company nor any other affiliated entity will act to engage D&T or accept from D&T any service that either has not been subjected to applicable preapproval process or that under SEC or other applicable rules would impair D&T's independence. All potential services are to be discussed with Mr. Gillam.

In connection with the foregoing paragraph, the Company agrees to furnish to D&T and keep D&T updated with respect to a corporate tree that identifies the legal names of the Company's affiliates, as defined in AICPA *Code of Professional Conduct* Interpretation No. 101-18 (e.g., parents, subsidiaries, investors, or investees) ("Company Affiliates"), together with the ownership relationship among such entities. Such information will be maintained in a database accessible by D&T in connection with their compliance with AICPA or other applicable independence rules.

Management will coordinate with D&T to ensure that D&T's independence as the Trusts' independent auditor is not impaired by hiring former or current D&T partners, principals, or professional employees for certain positions. Management will ensure that the Company, also has policies and procedures in place for purposes of ensuring that D&T's independence will not be impaired by hiring a former or current D&T partner, principal, or professional employee in an accounting role or financial reporting oversight role that would cause a violation of securities laws and regulations. Any employment opportunities with the Company for a former or current D&T partner, principal, or professional employee should be discussed with Mr. Gillam and approved by the Audit Committee before entering into substantive employment conversations with the former or current D&T partner, principal, or professional employee, if such opportunity relates to serving (1) as chief executive officer, controller, chief financial officer, chief accounting officer, or any equivalent position for the Company or in a comparable position at a significant subsidiary of the Company; (2) on the board of directors of the Company; (3) as a member of the Trust Committee or Audit Committee; or (4) in any other position that would cause a violation of securities laws and regulations.

For purposes of the preceding sections entitled "Independence Matters" and "Process for Obtaining Preapproval of Services", "D&T" shall mean Deloitte & Touche LLP and its subsidiaries; Deloitte Touche Tohmatsu Limited, its member firms, the affiliates of Deloitte & Touche LLP, Deloitte Touche Tohmatsu Limited and its member firms; and, in all cases, any successor or assignee.

APPENDIX C

COMMUNICATIONS WITH THE TRUST COMMITTEE

This Appendix C is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and the Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts, and Pacific Gas and Electric Company.

We are responsible for communicating with the Trust Committee significant matters related to the audits that are, in our professional judgment, relevant to the responsibilities of the Trust Committee in overseeing the financial reporting process.

In connection with the foregoing, we will communicate to the Trust Committee any fraud we identify or suspect that involves (1) management, (2) employees of the Company who have significant roles in internal control, or (3) other employees of the Company when the fraud results in a material misstatement of the financial statements. In addition, we will communicate with the Trust Committee any other matters related to fraud that are, in our professional judgment, relevant to their responsibilities. We will communicate to management any fraud perpetrated by lower-level employees of which we become aware that does not result in a material misstatement of the financial statements; however, we will not communicate such matters to the Trust Committee, unless otherwise directed by the Trust Committee.

We will also communicate to the Trust Committee matters involving the Trusts' noncompliance with laws and regulations that have come to our attention during the course of our audits, other than when such matters are clearly inconsequential.

We will also communicate in writing to management and the Trust Committee any significant deficiencies or material weaknesses in internal control (as defined in generally accepted auditing standards) that we have identified during the audits, including those that were remediated during the audits.

Generally accepted auditing standards do not require us to design procedures for the purpose of identifying other matters to communicate with the Trust Committee. However, we will communicate to the Trust Committee matters required by AICPA AU-C 260, *The Auditor's Communication with Those Charged with Governance*.

APPENDIX D

GENERAL BUSINESS TERMS

This Appendix D is part of the engagement letter to which these terms are attached (the engagement letter, including its appendices, the "engagement letter") dated December 10, 2019, between Deloitte & Touche LLP and the Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts, and Pacific Gas and Electric Company.

1. Independent Contractor. D&T is an independent contractor and D&T is not, and will not be considered to be, an agent, partner, fiduciary, or representative of the Company, the Trusts, the Audit Committee, or the Trust Committee.

2. Survival. The agreements and undertakings of the Company, the Trusts and the Trust Committee contained in the engagement letter will survive the completion or termination of this engagement.

3. Assignment and Subcontracting. Except as provided below, no party may assign any of its rights or obligations (including, without limitation, interests or claims) relating to this engagement without the prior written consent of the other parties. The Company, the Trusts and the Trust Committee hereby consent to D&T subcontracting a portion of its services under this engagement to any affiliate or related entity, whether located within or outside of the United States; provided, however that such subcontracting will not relieve D&T of any obligations to the Trusts or the Company hereunder. Professional services performed hereunder by any of D&T's affiliates or related entities shall be invoiced as professional fees, and any related expenses shall be invoiced as expenses, unless otherwise agreed.

4. Severability. If any term of the engagement letter is unenforceable, such term shall not affect the other terms, but such unenforceable term shall be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permissible the intent of the parties set forth herein.

5. Force Majeure. No party shall be deemed to be in breach of the engagement letter as a result of any delays or non-performance directly or indirectly resulting from circumstances or causes beyond its reasonable control, including, without limitation, fire, epidemic or other casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority.

6. Confidentiality. To the extent that, in connection with this engagement, D&T comes into possession of any confidential information of the Company or the Trusts, D&T shall not disclose such information to any third party without the Company's consent, using at least the same degree of care as it employs in maintaining in confidence its own confidential information of a similar nature, but in no event less than a reasonable degree of care. The Company, the Trusts and the Trust Committee hereby consent to D&T disclosing such information (1) as may be required by law or regulation, or to respond to governmental inquiries, or in accordance with applicable professional standards or rules, or in connection with litigation or arbitration pertaining hereto; (2) to the extent such information (i) is or becomes publicly available other than as the result of a disclosure in breach hereof, (ii) becomes available to D&T on a nonconfidential basis from a source that D&T believes is not prohibited from disclosing such information to D&T, (iii) is already known by D&T without any obligation of confidentiality with respect thereto, or (iv) is developed by D&T independently of any disclosures made to D&T hereunder; or (3) to contractors providing administrative, infrastructure, and other support services to D&T and subcontractors providing services in connection with this engagement, in each case, whether located within or outside of the United States, provided that such contractors and subcontractors have agreed to be bound by confidentiality obligations similar to those in this paragraph. To the extent that any information obtained by D&T from or on behalf of the Company or its employees in connection with the performance of services under the engagement letter relates to a resident

of Massachusetts and constitutes "Personal Information" as defined in 201 CMR 17.02 (as may be amended), D&T shall comply with the obligations of 201 CMR 17.00 et. seq. (as may be amended), entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth," with respect to such information. D&T shall promptly notify the Company if D&T becomes aware of any unauthorized access to or disclosure of confidential information of the Company or the Trusts.

7. Third Party Information Technology Controls Reports. Deloitte LLP ("Deloitte U.S.") has engaged a third party (the "Service Provider") to (i) apply procedures based upon a version of the Shared Assessment Program Agreed Upon Procedures with respect to certain of Deloitte U.S.'s information technology controls and to prepare a report with respect thereto (the "Shared Assessments Report"), and (ii) conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability, established by the American Institute of Certified Public Accountants (AICPA) ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC 2 Report"). Upon written request, Deloitte U.S. shall promptly provide Client with one copy of (i) the Shared Assessments Report, provided that Client executes any documentation required by the Service Provider to become a specified user thereof, (ii) the SOC 2 Report, or (iii), a report prepared by a third party that is designed to provide similar information as such reports. Client shall not disclose such reports, or refer to such reports in any communication, to any person or entity other than Client. In the event that Client has any questions regarding such reports, Deloitte U.S. shall make appropriate personnel reasonably available to discuss the contents thereof.

8. Code of Ethics and Professional Conduct. We acknowledge that we maintain a Code of Ethics and Professional Conduct. The D&T Code of Ethics and Professional Conduct (the "Code") may be found on www.deloitte.com under the Code of Ethics and Professional Conduct section under the Ethics & Independence section under the About section on that web site. The Code states that it is the obligation of all D&T personnel to know, understand, and comply with this Code.

9. Background Check Contract Requirements. Deloitte LLP and its subsidiaries (collectively the "Deloitte U.S. Firms") generally require that background investigations be conducted for all employees, partners, and principals at the time that they join the Deloitte U.S. Firms. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of such factors as whether the issues identified are job related or pose a risk to the Deloitte U.S. Firms or to their respective employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining one of the Deloitte U.S. Firms is a partner, principal or employee, and the level of the employee. While background investigations were not always performed on Deloitte U.S. Firms' personnel, and may not always have covered the same information, all background investigations of Deloitte U.S. Firms' personnel in the U.S. currently include the following, at a minimum:

- SSN verification: confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:
  - Federal courts
  - County courts
  - State repositories, where the state has made one available and it is reasonably accessible
- A national criminal record database search, including the state sex offender registries.

- Education confirmation: all education beyond high school confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

10. Information Security: D&T will comply with its security policies as set forth in Appendix F.

11. Successor/Predecessor Auditor Communication: In the event of a cessation of the client-auditor relationship, we agree to abide by professional standards with respect to communications between predecessor and successor auditors.

12. Dispute Resolution. Any controversy or claim between the parties arising out of or relating to the engagement letter or this engagement (a "Dispute") shall be resolved by mediation or binding arbitration as set forth in the Dispute Resolution Provision attached hereto as Appendix E and made a part hereof; provided, however, to the extent there is an active lawsuit that was initiated by a third party against the Company, the Trusts or D&T ("third party action"), the Company, the Trusts or D&T, as the case may be, may seek resolution of a related Dispute (such as a claim for contribution) against D&T, the Trusts, or the Company, as the case may be, in such third party action.

APPENDIX E

DISPUTE RESOLUTION PROVISION

This Appendix E is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and the Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts, and Pacific Gas and Electric Company.

This Dispute Resolution Provision sets forth the dispute resolution process and procedures applicable to the resolution of Disputes and shall apply to the fullest extent of the law, whether in contract, statute, tort (such as *negligence*), or otherwise.

Mediation: All Disputes shall be first submitted to nonbinding confidential mediation by written notice to the parties, and shall be treated as compromise and settlement negotiations under the standards set forth in the Federal Rules of Evidence and all applicable state counterparts, together with any applicable statutes protecting the confidentiality of mediations or settlement discussions. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR"), at the written request of a party, shall designate a mediator.

Arbitration Procedures: If a Dispute has not been resolved within 90 days after the effective date of the written notice beginning the mediation process (or such longer period, if the parties so agree in writing), the mediation shall terminate and the Dispute shall be settled by binding arbitration to be held in San Francisco, California. The arbitration shall be solely between the parties and shall be conducted in accordance with the CPR Rules for Non-Administered Arbitration that are in effect at the time of the commencement of the arbitration, except to the extent modified by this Dispute Resolution Provision (the "Rules").

The arbitration shall be conducted before a panel of three arbitrators. The Company and the Trusts, on the one hand, and Deloitte & Touche LLP, on the other hand, shall each designate one arbitrator in accordance with the "screened" appointment procedure provided in the Rules and the two party-designated arbitrators shall jointly select the third in accordance with the Rules. No arbitrator may serve on the panel unless he or she has agreed in writing to enforce the terms of the engagement letter (including its appendices) to which this Dispute Resolution Provision is attached and to abide by the terms of this Dispute Resolution Provision. Except with respect to the interpretation and enforcement of these arbitration procedures (which shall be governed by the Federal Arbitration Act), the arbitrators shall apply the laws of the State of California (without giving effect to its choice of law principles) in connection with the Dispute. The arbitrators shall have no power to award punitive, exemplary or other damages not based on a party's actual damages (and the parties expressly waive their right to receive such damages). The arbitrators may render a summary disposition relative to all or some of the issues, provided that the responding party has had an adequate opportunity to respond to any such application for such disposition. Discovery shall be conducted in accordance with the Rules.

All aspects of the arbitration shall be treated as confidential, as provided in the Rules. Before making any disclosure permitted by the Rules, a party shall give written notice to all other parties and afford such parties a reasonable opportunity to protect their interests. Further, judgment on the arbitrators' award may be entered in any court having jurisdiction.

Costs: Each party shall bear its own costs in both the mediation and the arbitration; however, the parties shall share the fees and expenses of both the mediators and the arbitrators equally.

APPENDIX F

INFORMATION SECURITY STATEMENT

This Appendix F is part of the engagement letter dated December 10, 2019, between Deloitte & Touche LLP and the Nuclear Facilities Decommissioning Master Trust Committee on behalf of itself and the Trusts, and Pacific Gas and Electric Company.

Overview

Deloitte LLP and/or its affiliates ("Deloitte") has developed and implemented an Information Technology ("IT") infrastructure that is designed to generally align with industry standards. The security boundary of the IT infrastructure includes Deloitte- issued laptops, as well as infrastructure and applications, such as databases, document collaboration, email, and backup systems. The IT infrastructure security controls and associated information security processes were developed to protect confidential information while making it available in appropriate circumstances. A summary of such policies, controls, and associated processes is set forth below.

Purpose

The purpose of this Information Security Statement is to provide an overview of Deloitte's IT security practices that are in effect as of the recent published date of this document (4/11/2019). From time to time, Deloitte may modify or update these policies, controls and associated processes. Deloitte shall not be under any obligation to notify any client of any such change to its policies, controls and associated processes.

Cyber Security

Deloitte's Chief Information Security Officer ("CISO") oversees the Cyber Security team, which provides assistance in the following areas:

- eDiscovery Forensic Investigations:
  - Manages the end-to-end process of collecting data requested by the Office of General Counsel ("OGC") for legal and regulatory matters
  - Works with OGC and the Talent organization to conduct internal investigations on misuse of data resources and manages security incident responses
  - Acquires, documents, and preserves digital evidence for computer forensics
- Risk & Compliance:
  - Leads and manages the vendor security program and privacy impact assessment process
  - Collaborates with client service leaders and OGC in responding to client security inquiries and security agreements
  - Leads Deloitte's third party audit and assessment (e.g., SOC2 and Shared Assessments Agreed Upon Procedures)
  - Leads Deloitte's security awareness efforts and assists with global security awareness efforts

- Responsible for exceptions to security policies and standards

- Cyber Defense:
  - Monitors, analyzes, and responds to all types of system, device, and application events, such as user activity, firewalls, IDS/IPS, antivirus, and vulnerabilities
  - Identifies, rates, and remediates potential security vulnerabilities of applications and systems
  - Understands which Deloitte systems are used, how, and by whom and uses this information to protect the organization from potential threats

- Data Protection:
  - Reviews emerging technologies, security architecture, and proposals for improvements
  - Leads the identity management program
  - Leads Federal support and maintains FedRAMP certifications.
  - Members of the Cyber Security team hold various industry security- and audit-based certifications (e.g., CISSP, CISM, CISA, ISSM, CRISC, CEH, ISO 27001 Lead Auditor, and OSCP).

Information Security Program

Deloitte maintains a comprehensive information security program, which includes policies, standards, procedures and guidelines. The information security program is informed by several industry-standard guidelines and best practices including ISO27001, COBIT, ITIL, American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC2"), and the Shared Assessments Program (formerly known as the "BITS Financial Institution Shared Assessments Program").

Deloitte's IT leadership meets on a regular basis to consider strategic and tactical direction for the information security program, and its policies, standards, procedures and guidelines.

Information security policies are drafted with input from internal information security stakeholders and are based upon industry standard practices. The drafts are reviewed and approved by Deloitte's Cyber Security leadership, OGC, the Office of Confidentiality and Privacy, the CISO and Deloitte's Chief Information Officer. Once approved, the policies are published on Deloitte's intranet and communicated to personnel.

Certification

Deloitte has established and operates an Information Security Management System that manages its client confidential information (ISMS). The ISMS has been certified by an independent third party that it complies with the requirements of the International Information Security Management System Standard ISO/IEC 27001.

On-Site Security Assessments

In an effort to protect and minimize risk to Deloitte's client data, in lieu of permitting individual clients to perform independent security assessments of Deloitte's information security program,

each year Deloitte engages an independent third-party auditor ("Third Party") to (i) conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability established by the AICPA ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC2 Report"), and (ii) apply procedures based upon a version of the Shared Assessments Program Agreed Upon Procedures (the "Shared Assessments AUPs") with respect to certain of Deloitte's information technology controls and to prepare a report with respect thereto (the "Shared Assessments Report").

SOC2 Report

The SOC2 Report includes the Third Party's opinion on the fairness of the presentation of the description of Deloitte's systems in management's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on the Third Party's examination. The SOC2 Report also includes a description of Deloitte's systems and controls, and a description of the Third Party's criteria, test procedures, and the results of such tests. The SOC2 Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the SOC2 Report.

Shared Assessments Report

The Shared Assessments Report is used to assist Deloitte management in evaluating certain IT controls related to the security of Deloitte's client data. The Shared Assessments Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the Shared Assessments Report and has executed an access letter with the Third Party.

The Shared Assessments Program includes the Agreed Upon Procedures (which are a list of security control objectives) and the Standardized Information Gathering ("SIG") questionnaire. Detailed information about the Shared Assessments Program can be found at http://www.sharedassessments.org/. The Shared Assessments Program defines specific controls and objectives as well as the procedures for verifying those controls. The Agreed Upon Procedures address the following controls areas:

- Risk management
- Information security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance
- Privacy

Awareness and Training

Deloitte has implemented training and awareness programs for its personnel related to information-security, confidentiality and privacy policies and practices. Deloitte personnel are required to complete a confidentiality, privacy, and information security awareness training during the new-hire onboarding process, as well as an annual update course thereafter. Deloitte

personnel are presented with an information security policy awareness statement via Deloitte's intranet two times each year, which they are required to acknowledge within two weeks of the statement's release.

Deloitte has a dedicated security awareness committee. The committee is responsible for developing ideas to enhance Deloitte's awareness of security risks and issues through policy development and training. The committee is comprised of delegates from Deloitte's Cyber Security leadership, National Office of Security, Office of Confidentiality and Privacy, CISO, National Quality Risk Management, Talent, and OGC, and from Deloitte Touche Tohmatsu Limited's Global Information Security Office, who regularly meet to discuss new or recurring security issues, devise strategies and implementation plans, and provide progress reports on existing projects.

Management and Protection of Confidential Information

Deloitte is committed to protecting the confidential information, including Personally Identifiable Information (PII), of our clients, our organization and the third parties with whom we work. "Confidential Information" refers to any information not generally available to the public, in any form, that Deloitte receives or creates in the course of business. To support this commitment, Deloitte has established the Office of Confidentiality and Privacy which is responsible for setting guidelines, developing procedures, and providing consultation and training on the management of Confidential Information.

The Office of Confidentiality & Privacy has also developed the "Confidential Information Program" for the proactive management and protection of Confidential Information and is responsible for implementing the Confidential Information Program across Deloitte. The Confidential Information Program consists of processes, technology controls, training, and communications that help our professionals to improve their awareness of risks associated with Confidential Information and their ability to properly manage and safeguard Confidential Information.

The Confidential Information Program

The Confidential Information Program consists of processes and activities that are performed throughout the engagement lifecycle to manage and protect Confidential Information.

Client account and engagement teams in the Confidential Information Program generally do the following:

- Appoint a data manager responsible for overseeing program activities;
- Develop and maintain a Confidential Information management plan to document the Confidential Information management strategy and safeguards employed;
- Develop and deliver Confidential Information onboarding training that outlines the protocols that team members must follow when accessing, storing, using, transferring, and disposing of Confidential Information;
- Implement physical, administrative, and technical safeguards identified in the Confidential Information management plan to proactively manage risk; and
- Complete all other required confidentiality training as applicable.

Deloitte also has an insider threat program in which Deloitte conducts active monitoring of insider threats. Insiders are defined as personnel and contractors who, based on their access to certain systems and information, could adversely affect the brand, reputation and/or business of Deloitte or its clients. Leveraging potential risk indicators, the insider threat program monitors persons of interest across a broad risk spectrum, including workplace

violence, espionage, fraud, and theft of intellectual property and Confidential Information. Analytic and cognitive technologies are used to help identify indicators of poor risk-culture fit and determine corresponding strategic tactics and mitigation strategies to align our sub-cultures

Data Privacy

Deloitte is committed to protecting our clients' Personally Identifiable Information ("PII"). Deloitte has a data privacy policy, applicable procedures, and personnel dedicated to making sure we comply with applicable data privacy laws and regulations. We regularly monitor for changes in data privacy laws and regulations and adjust our policies and procedures when appropriate. Additionally, we have instituted an annual review process across all Deloitte business areas to verify compliance with our privacy policy and procedures.

- Deloitte has policies and procedures that protect PII and support compliance with US and the European Union (EU) legal requirements relating to the transfer and processing of PII, including personal health information.

- Deloitte adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to PII that is transferred from the European Economic Area and Switzerland to the United States.

- Deloitte is not a "Covered Entity" as defined under the Health Insurance Portability and Accountability Act, as amended ("HIPAA"). Therefore, Deloitte is generally not required to, and does not, comply with the obligations of a Covered Entity. However, when Deloitte acts in the capacity of a "Business Associate" to our clients, as such role is defined under HIPAA, Deloitte is required to comply with the obligations of a Business Associate under HIPAA. Deloitte has implemented policies, procedures, and controls that facilitate compliance with those obligations.

- Deloitte utilizes a Privacy Impact Assessment (PIA) process for new systems, changes to existing systems and high-risk business processes that access, transfer or store PII.

- In support of the Privacy by Design concept, Deloitte has incorporated privacy and confidentiality requirements into our secure systems development lifecycle (SSDLC) for internally developed systems so that these requirements are considered early and often throughout the lifecycles of technology projects using a risk-based approach.

Confidentiality and Privacy Incident Management

Deloitte has instituted an integrated incident response process designed to facilitate prompt reporting and resolution of incidents. Our confidentiality and privacy incident response process is characterized by the following:

- Centralized reporting of actual or suspected incidents to a Help Desk, which is available 24/7 with access via a toll-free number;

- Training and awareness programs focused on helping personnel understand immediate steps to be taken in case of actual or suspected incidents;

- Established roles and responsibilities for incident management and response including involving the appropriate consultation resources across the Deloitte organization, as applicable to the specific matter;

- Documented processes to help gather incident facts, initiate response activities, engage incident response teams, escalate incidents and alert appropriate leaders, based on the nature of the specific incident;

- Consultation among the relevant parties regarding the need for a corrective action plan;
- Development, as appropriate, of action plans, including any required communications, as well as actions to mitigate the risk of a future recurrence; and
- Post-incident follow-up process to analyze root causes and integrate lessons learned.

IT Continuity Management

Deloitte maintains an active disaster recovery and business continuity program which helps to continue delivering information-technology-related services should a disruption occur. Deloitte's program includes the following basic activities:

- Business continuity planning for IT infrastructure support staff;
- Business impact assessments to help define criticality of processes and systems related to recovery time objectives;
- Disaster recovery planning of our technology through multiple failover capabilities;
- Implementation of resilient architectures where technology allows;
- Risk assessments as part of continual service improvement, with countermeasures identified and implemented for the newest scenarios; and
- Internal review process for maintaining the quality of plans and services.

The business continuity program ("BCP") and plans include emergency-response business procedures, which go into effect following the occurrence of a disaster or other unplanned interruption.

Disaster recovery ("DR") plans include technical and business contact call lists, as well as notification and escalation information and architecture diagrams. Where pertinent, third-party information is also included. Recovery time objectives and recovery point objectives are documented and tested for each plan.

BCP/DR plans for critical infrastructure are subject to review and testing every 12 months with industry standard testing methods.

Risk assessment test scenarios vary based on business sensing and technology security. Test results are reviewed and recorded.

In summary, Deloitte has a comprehensive disaster recovery and business continuity program that is designed to provide for the continuity of essential IT business functions and critical business processes following the occurrence of a disaster or other unplanned interruption impacting Deloitte's IT infrastructure.

Business Continuity Management

Deloitte takes disaster and contingency planning very seriously, including planning for events that impact its people and/or its facilities. Deloitte's business continuity planning addresses issues such as, communications, travel, resource allocation, technology needs, and alternate work sites. Response procedures assess the well- being of personnel, provide for the continuity of essential business functions, and utilize recovery procedures for the restoration of critical business processes. Cross-functional teams are identified to manage potential disruptive events, emergency situations or disasters. Each Deloitte office has a local crisis management team to handle smaller, localized events

impacting a single location. For larger events or those that are not specific to a single location or geography, an experienced national incidents support team is assigned ("National Incident Support Team"). A national crisis council handles incident that rise to the level of a true crisis requiring strategic involvement and decision-making.

Cross-functional teams are identified and documented in the plans to include representation of key stakeholders from the following areas:

- Client Services
- Office Services/Operations/Facilities
- Office of Security
- Human Resources and Benefits
- Information Technology Services
- Procurement and travel
- Communications
- Risk Management

Deloitte has designed an impact-driven approach, which focuses on the impacts of an event, emergency, or crisis, rather than specific scenarios. Each type of situation could have an impact on our people, our facilities, our technology, or our clients. Each type of situation could require communications, whether internal or external. The team-based, impact-driven approach utilized by Deloitte provides the best resources to assess and address the impacts of an event.

Deloitte has developed a specific plan to address the impacts and continuity of operations in light of a pandemic ("Pandemic Plan"). The Pandemic Plan and related governance model is aligned with the crisis management and business continuity processes, including the use of the National Incident Support Team, but is supplemented by additional members of a Pandemic Response Committee. The Pandemic Response Committee monitors potential pandemic developments and would oversee implementation of specific pandemic action steps based on the severity of the pandemic, including targeted communications that would be issued internally and externally, and identification of critical people and resources.

Limits of Business Continuity and Pandemic Planning

Due to the significant uncertainties associated with a possible flu pandemic or other disaster, Deloitte can make no representations or warranties, nor provide any assurances, that its plans will be adequate to respond to any possible consequences, or that the plans of any third parties to deal with a possible flu pandemic or other disaster are or will be sufficient to address any situations or problems that might arise during a pandemic or other disaster. Deloitte's objective is to prepare for a possible flu pandemic or other disaster based on the information and data that it has at this time, and to possibly modify those plans as it believes conditions or facts may warrant. Every organization needs to develop its own preparedness plan based on its specific circumstances, business functions, and operational factors. Consequently, a plan developed for one function or business cannot be expected to address the potential issues that may be faced by another business enterprise. Because business continuity and disaster recovery plans and documentation contain information about Deloitte that is proprietary and confidential, Deloitte does not provide third parties with copies of such plans or documentation.

Human Resources Security

Upon hire, all personnel agree to comply with Deloitte's policies, including those relating to information security, confidentiality and privacy. In addition, all Deloitte personnel are required to complete security awareness training during the new hire onboarding process.

Background Checks for U.S. Personnel

Deloitte generally requires that background investigations be conducted for partners, principals

and all employees at the time that they join Deloitte. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of whether the issues identified are job-related or pose a risk to Deloitte or to its employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining is a partner or principal and the level of the employee. While background investigations were not always performed on Deloitte personnel, and may not always have covered the same information, all background investigations of Deloitte personnel in the U.S. currently include the following, at a minimum:

- SSN verification: confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:
    - Federal courts
    - County courts
    - State repositories, where the state has made one available and it is reasonably accessible
- A national criminal record database search, including the state sex offender registries.
- Education confirmation: education beyond high school confirmed
- Employment confirmation: professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

Background checks for Personnel of Deloitte entities located in India ("U.S. India")

The type of background investigation performed depends on whether the individual joining U.S. India is a partner, principal, or employee, and the level of the employee. While background investigations were not always performed on U.S. India's personnel and may not always have covered the same information, all background investigations of U.S. India personnel currently include the following, at a minimum:

- Identity Verification, where possible
- Criminal checks: check all relevant court records for a five year period
- Education confirmation: all university level education is confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, including India specific and global databases
- Professional licenses: confirm relevant professional licenses

Physical and Environmental Security

Only authorized personnel with a Deloitte-issued electronic badge are granted access to Deloitte's facilities. Procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the facilities. Deloitte data centers are further restricted to only those personnel with the need to access restricted areas. Data centers have the following physical security measures:

security guards, man-trap doors at primary entrance, multi-factor authentication (Deloitte-issued electronic badge and biometric readers) at secondary entrance, video cameras, and sign-in and sign-out sheets for escorted visitors.

The electricity, water, and temperature controls are all pre-approved for use by the facilities administrators in the data centers. Each utility has a control in place to monitor its usage and to notify an administrator in case of failure. Automatic emergency lighting is installed in areas necessary to maintain personnel safety.

Emergency exits are located in appropriate places in Deloitte facilities. Automatic fire suppression systems have been installed to protect the facilities. In data centers, the primary system is HFC-125 chemical based and activated via multiple smoke detectors, and the second type is pre-action hydronic, and the detection method is temperature. Master water shut-off valves are present. Temperature and humidity controls have been implemented to protect against temperature fluctuations in all areas of the data centers containing IT equipment.

Risk Management

Deloitte has a risk management program that monitors possible threats and vulnerabilities to information technology assets. Risk assessment(s) are performed annually and when there are significant changes to infrastructure, technology or environment. There are several control domains defined for risk assessment. These control domains are derived from industry standard practices and frameworks. For each control domain, implemented controls are identified and tailored and their effectiveness assessed for risk management. Risks that are not at an acceptable level are remediated or mitigated.

Vendor Hosting and Processing

Deloitte has arrangements with vendors who provide Deloitte with certain software-as-a service and hosting services. Deloitte selects and retains these vendors based on, among other qualities, their capability to maintain safeguards for the systems, software and information at issue that are consistent with leading industry security practices. Deloitte requires these vendors to implement and maintain such safeguards.

Vendor Assessment Process

The Vendor Assessment process is designed to reduce vendor-related risk by:

- Building a repository of acceptable vendors;
- Assessing the security posture of vendors;
- Tracking remediation of identified issues; and
- Reviewing and assisting with vendor contracts with respect to obligations relating to Deloitte's information security program.

Asset Management

Deloitte has an asset management team that is responsible for oversight and management of Deloitte assets and inventory throughout its lifecycle. There are tools and controls in place that manage hardware and software assets. Deloitte has policies and procedures in place to manage licensed software and security controls to deter prohibited software from being installed and/or used. A software and hardware inventory system is maintained, which identifies hardware and software components used within Deloitte information systems. Multiple controls are used to manage the configuration baselines, including mobile device management. These controls are supported by automated tools that provide configuration and inventory information on a continuous basis specific to configuration compliance, known vulnerabilities, inventory by Internet Protocol address ("IP address")/device name and asset operational and connection status.

Access Control

Access to Deloitte information contained on Deloitte IT systems is granted on a need-to-know basis and must be approved by the Deloitte data owner.

Vendor and contractor access is requested through procedures that involve Deloitte's Talent and Technology groups. Upon approval, the vendor user accounts are created in a controlled domain organizational unit giving the access necessary to perform their defined duties. Vendor and contractor access is granted on a temporary basis based on business need.

For certain systems, remote access is provided via a Secure Sockets Layer ("SSL") Virtual Private Network ("VPN") using two-factor authentication with account activity being logged to Deloitte's logging/alerting mechanism. Depending on the level and type of access required, the SSL VPN solution provides a virtual session or web interface with access into the needed application(s) or platform.

For web-based applications that contain or provide access to sensitive internal or client data (including VPN), Multi-Factor Authentication (MFA) has been enabled. Verification options include phone call, text message, or mobile application.

Privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into role-based groups (e.g., key management, network, system administration, database administration, and web administration).

Identification and Authentication

All users must authenticate to the Deloitte network using a unique user identification ("ID") and a strong password prior to gaining access to the information system.

Deloitte strong passwords contain the following characteristics:

- Passwords are required to be at least ten (10) characters in length and contain at least three of the following four elements: (1) westernized Arabic numbers (e.g., 2,5,9), (2) non- alphanumeric characters (e.g., #, %, !, %, @, ?, -, *), (3) English uppercase letters (e.g., A, B, C), and/or (4) English lowercase letters (e.g., a, b, c)
    - Passwords are not permitted to contain:
        - parts of the users' username, first name, or last name
        - dictionary words with or without (i) numbers or special characters at the beginning or end, or (ii) letters, numbers, or character exchanges (e.g., Summer2017, ?Happyman, H3llofr!end?)
        - words or numbers connected with users such as family names, petnames, birthdays, addresses, or phone numbers
        - common terminology, acronyms, or names associated with the Deloitte or its clients
        - any variation of 'Deloitte' or 'Password' (e.g., Deloitte12, P@ssw0rd12, Pa$$w0rd!2)
        - any sequencing of letters and numbers that follow the order of a keyboard (i.e., keyboard walk patterns such as 1234qwerASDF, 1qazXSW@3edc)

Additional Password Safeguards

The following additional password related safeguards are enforced:

- Users are not permitted to reuse their previous twenty-four passwords
- Passwords expire every 90 days

- There is a password lockout threshold after 6 invalid logon attempts

System Security

System and Communications Protection

An intrusion prevention system ("IPS") is employed at the point of entry to the Deloitte network environment. The logs for the IPS, firewall, and VPN are sent to a log aggregator. Access control lists are placed on firewalls controlling the inbound and outbound flow of traffic. Traffic is denied by default unless approved by the gateway protocols as configured and approved by the Deloitte security team. A demilitarized zone ("DMZ") and trusted zones are used to segment traffic to areas that are protected in accordance with the accepted risk levels.

System and Information Integrity

Firewall, IPS, and VPN audit logs are sent to the log aggregator, which checks for abnormal activity and anomalous behavior that would trigger an information security review. Hardware and software checks are done by automated tools with identified alert levels that trigger a notification to the system administrators in case of a system flaw. Anti-virus and malware protection is managed by enterprise policy and distributed by a server located in the environment periodically. Anti-virus is configured to scan external devices attached to the information system as well as email traffic.

Data Back-up

Deloitte systems are scheduled for daily backup and two iterations of data through redundant data mirroring: one onsite and one offsite. If a system backup is interrupted for any reason, it will resume on the alternate site where it left off. A reputable vendor is utilized for offsite backup storage and disposal. All backup media is encrypted prior to shipment to the vendor and a controlled process exists for turnover. The vendor is subject to obligations of confidentiality. The vendor has security practices in place and uses a tracking application for all media it handles on Deloitte's behalf. Deloitte is provided with inventory reports of the media and chain-of-custody. The vendor stores the media in a secure, environmentally-controlled storage facility.

Information Systems Acquisition, Development and Maintenance

Security Planning

The Deloitte information security program, applicable policies, standards, standard operating procedures and guidelines are reviewed annually and updated as necessary.

Acquisition of System and Services

Deloitte does not acquire IT systems or services until Cyber Security has reviewed the product or service to determine whether it meets internal guidelines with respect to security and encryption. Software installation requests are submitted for risk assessment and approval. Software is not implemented unless it meets applicable Information Technology Services ("ITS") standards. There is a Change Control Board ("CCB") that discusses any changes that may affect the security posture of the environment and documents all proposed upgrades or modifications to the environment, assets and infrastructure.

Application Development

Deloitte follows secure coding best practices during the system development lifecycle for Deloitte applications. Deloitte's applications undergo security reviews, testing and vulnerability scans prior to being placed in production.

Change Control

Deloitte has a change management process in place for its IT systems. Proposed changes are submitted, tested, and reviewed during regularly scheduled CCB meetings. Approved changes are tested and vulnerability scans are performed prior to deployment. Deployment windows are scheduled to minimize the impact to Deloitte's operations. Back-out plans are in place should they be needed.

Patch Management

Deloitte has a patch-management program and supporting tools in place that are managed by an internal patch management team ("PMT"). Vendor and industry-accepted alert lists are monitored for new patches. Patches are reviewed by the PMT at regularly scheduled meetings and are rated for deployment based on assessed severity levels. Emergency patch management meetings are called when needed.

Vulnerability Management

Deloitte's network undergoes penetration testing and vulnerability scans performed by Deloitte's Cyber Defense team. Penetration tests are performed annually on the network infrastructure's external perimeter by Deloitte's Cyber Defense team. Vulnerability scanning is performed weekly on the network infrastructure's internal and external perimeter by Deloitte's Cyber Defense team.

Maintenance

Deloitte ITS performs software and hardware maintenance on Deloitte's environment servers.

Information system backups are performed daily. Performance reports are initiated through automated tools that specify certain levels of performance to trigger the generation of the report (i.e., % of CPU processor utilization, etc.).

Third-party contractor maintenance personnel must be approved prior to receiving access to the information system servers. Third party maintenance personnel are escorted into the facility and accompanied during the period of access. A log is maintained which documents the name, date, length of time, justification, and escort name for each maintenance individual who is granted access to the information system(s).

Information Security Incident Management

Deloitte has built an integrated incident response team that brings together the appropriate subject matter experts from various cross-functional disciplines to address each specific incident. The Security Incident Response Procedures ("Procedures") describe how various types of incidents are handled. The Procedures identify key resources and communications that will take place based on various incident types. The Procedures identify to whom suspected incidents should be reported and describe the escalation path from the entry point in the process through fruition. Security awareness training is in place to educate Deloitte personnel of their responsibilities concerning security incidents. Each incident is logged, and the relevant facts are captured for analysis and reporting. When necessary, data related to the incident is maintained in a forensically sound

manner and appropriate chain-of-custody is documented.

The incident response team has a variety of tools available to assist them in the analysis of incidents. These include standard security tools from software and hardware providers as well as commercial forensic tools specifically targeted for such matters.

Information security incident procedures are executed periodically so the teams remain prepared for response should the need arise. At the completion of each significant incident, a post-incident review is conducted to identify any areas for improvement as well as lessons learned. These findings are used to adjust, enhance or improve the procedures.

Compliance

System Audit and Accountability

System audit logs and records are created to monitor the following

- anti-virus services
- intrusion prevention services
- remote access services, web proxy services
- domain authentication
- router events
- firewall events
- VPN access
- application logs
- operating system logs
- privileged access logs

System audit logs are maintained to support analyses and investigations. Logs are maintained for a period of one (1) year. Logs may also be preserved based on legal or regulatory requirements.

System audit log content includes: (i) date and time of the security event; (ii) the component of the information system (e.g., software component, hardware component) where the security event occurred; (iii) type of security event; (iv) unique user/subject identity; and (v) the outcome (success or failure) of the security event.

System Audits

Deloitte's internal audit team periodically performs internal audits on various aspects of Deloitte's systems, processes, and policies.

Application Configuration Management

Software baseline requirements are created in accordance with Deloitte policies and standards. Software is tested against the baseline requirements prior to being placed in the production environment. Continued monitoring and change management processes are conducted while in operation.

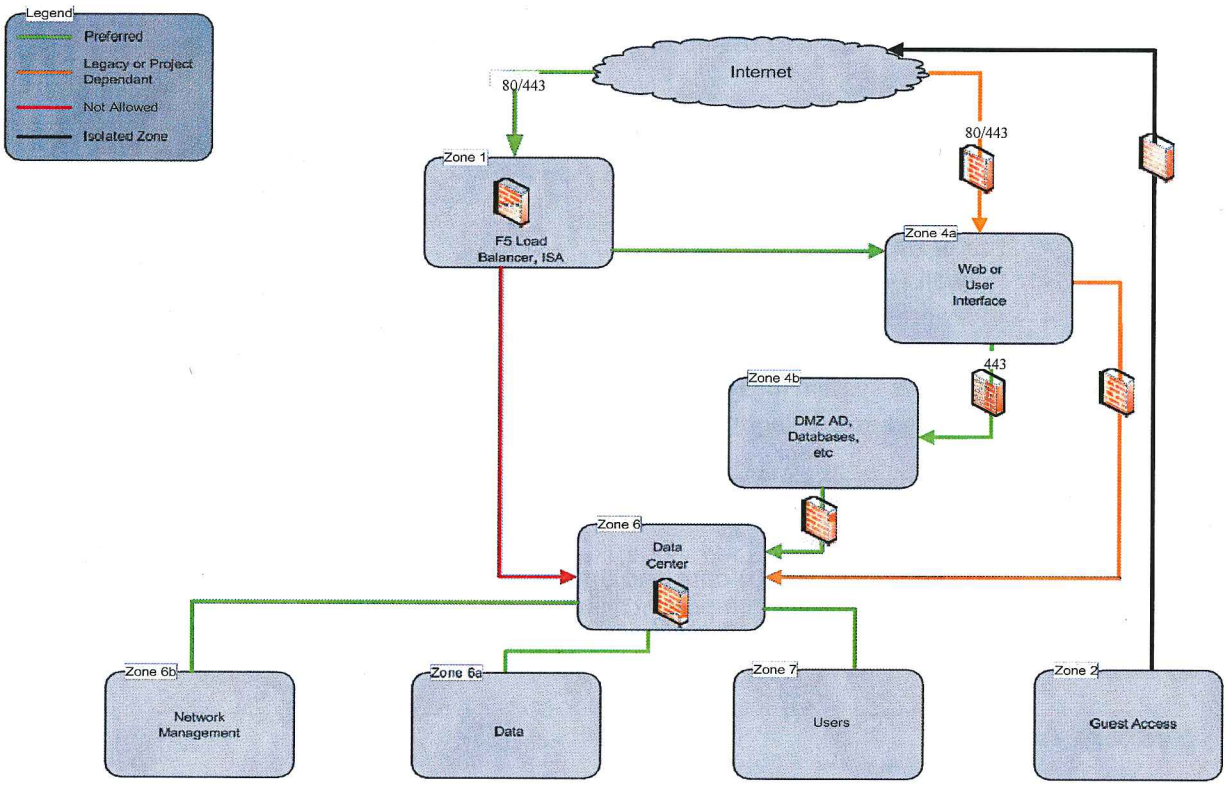
Wireless Access

Deloitte supports an internal wireless network within the organization. A wireless-security and acceptable- use policy is in place. Only Deloitte-approved access points will be connected to Deloitte's network.

- For wireless access to Deloitte's networks, personnel are required to use Wi-Fi Protected Access (WPA2 or stronger protection) where it is available.
- For the convenience of visitors, clients, or guests, a guest wireless network providing controlled access to the Internet may be made available in Deloitte's facilities.

Data Flow Diagram

Zone Flow – Basic Rules for Zone Flow



Data Protection

Deloitte personnel receive training on the proper handling of PII. In instances where Deloitte may transmit client PII outside of the Deloitte environment, Deloitte requires transmission of such data in an encrypted format.

Media Protection

Secure printing is available at multiple locations within each Deloitte office that requires the usage of a Deloitte-issued electronic smartcard badge to enable the print job. Further, Deloitte issues encrypted USB drives to its personnel that meet the encryption standards outlined in Federal Information Processing Standard ("FIPS") 140-2. In addition, software has been deployed to Deloitte-issued IT assets as part of the standard application toolset that allows the creation of encrypted WinZip files (FIPS 197 compliant).

Deloitte has implemented a technical control that encrypts data written/copied to external USB devices which can only be read by a Deloitte machine.

Laptops are encrypted and are required to be physically secured at all times. Physical access to servers is restricted to authorized parties. Magnetic drives are wiped/over-written with a minimum of three passes with a media sanitization tool prior to being released for re-use and disposal.

Deloitte has employed the following methods of PDA protection: 1) forced access PINs; 2) remote wipe in the event of 10 incorrect pin attempts; 3) remote wipe if the PDA is reported as lost or stolen; 4) encryption; and 5) an installed mobile device management tool.

Data Destruction

Policies and practices are in place with regard to the destruction of confidential information and PII that vary depending on type of media on which such information is stored. Deloitte is aligned with the National Institute for Standards and Technology's ("NIST") guidelines for media sanitization. For example, hard disks, CD/DVD, USB drives are required to be wiped using a disk cleaning tool, while tapes are required to be destroyed at end-of-life. Paper containing such information is required to be shredded.

Encryption

Whole-disk encryption has been deployed on Deloitte-issued laptops. Deloitte's laptops have deployed encryption with the 256-bit Advanced Encryption Standard ("AES") algorithm.

Deloitte has deployed encrypted USB drives intended for use in transporting sensitive or confidential data. This encryption method is FIPS 140-2 compliant.

WinZip is installed on all Deloitte-issued laptops. This encryption method is FIPS 197 compliant.

Additionally, Deloitte Internet email gateways are configured to attempt to transmit all email in an encrypted manner, using opportunistic TLS encryption, if the recipient of the transmission can support such encryption methodology. If TLS is enabled on the recipient email gateway, the email will be encrypted between the Deloitte gateway and the recipient gateway. TLS encryption can also be enforced when agreed with the recipient organization. This encryption method is FIPS 140-2 compliant.

Data in transit is protected by secure TLS using certificates with minimum 2048-bit RSA key and SHA2 signing when using Deloitte secure websites and file transfer services.

Secure File Transfer Protocol ("SFTP") is an available option for the transfer of client data. SFTP securely encrypts and compresses files during transmission. This encryption method is FIPS 140-2 compliant.

Records Management

Deloitte maintains and retains records in accordance with applicable legal and regulatory requirements and professional standards. Specific areas of focus include:

- Facilitating compliance with external requirements and internal policies and practices pertaining to record retention;
- Managing recordkeeping critical to the operation of our business and service to our clients;
- Designing and implementing records management technology, tools, and standard processes;
- Coordinating the proper handling of files on legal hold due to legal, tax or regulatory preservation requirements; and
- Maintaining a strong, compliance-focused records and information management governance organization.